OpenManage Integration for VMware vCenter User's Guide Version 2.0

Notes, Cautions, and Warnings

NOTE: A NOTE indicates important information that helps you make better use of your computer.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

© 2013 Dell Inc.

Trademarks used in this text: Dell™, the Dell logo, Dell Boomi™, Dell Precision™ , OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™, Force10™ and Vostro™ are trademarks of Dell Inc. Intel®, Pentium®, Xeon®, Core® and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. AMD® is a registered trademark and AMD Opteron™, AMD Phenom™ and AMD Sempron™ are trademarks of Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista® and Active Directory® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat® and Red Hat® Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® and SUSE® are registered trademarks of Novell Inc. in the United States and other countries. Oracle® is a registered trademark of Oracle Corporation and/or its affiliates. Citrix®, Xen®, XenServer® and XenMotion® are either registered trademarks or trademarks of Citrix Systems, Inc. in the United States and/or other countries. VMware®, vMotion®, vCenter®, vCenter SRM™ and vSphere® are registered trademarks or trademarks of VMware, Inc. in the United States or other countries. IBM® is a registered trademark of International Business Machines Corporation.

2010 -13

Rev. A00

Contents

1 Introduction....9
OpenManage Integration for VMware vCenter Features....9

2 Understanding How to Configure or Edit the OpenManage Integration for VMware vCenter....11
Configuration Wizard Welcome Page....11
vCenter Selection....11
Creating A New Connection Profile using the Initial Configuration Wizard....12
Scheduling Inventory Jobs [Wizard]....13
Running A Warranty Retrieval Job [Wizard]....14
Configuring Events And Alarms [Wizard]....14

3 About VMware vCenter Web Client Navigation....17
Navigating to the OpenManage Integration for VMware vCenter Inside the VMware vCenter....17
Understanding Icon Buttons....17
Locating the Software Version....18
Refreshing the Screen Content....18
Viewing the OpenManage Integration for VMware vCenter Licensing Tab....18
Opening Online Help....19
Finding Help and Support....19

4 Connection Profiles....21
Viewing Connection Profiles....21
Creating A Connection Profile....21
Editing a Connection Profile....23
Refreshing A Connection Profile....24
Deleting A Connection Profile....24
Testing a Connection Profile....25

5 Inventory History....27
Viewing Inventory History....27
Changing Inventory Job Schedules....28
Running an Inventory Job Now....28

6 Warranty History....29
Viewing Warranty History....29
Modifying a Warranty Job Schedule....30
Running a Warranty Job Now....30

7 Console Administration....31
Using the Administration Console....31
Registering a vCenter Server....31
Modifying The vCenter Administrator Login....32
Updating The SSL Certificates For Registered vCenter Servers....32
Uninstalling the OpenManage Integration for VMware vCenter From VMware vCenter....32
Uploading a OpenManage Integration for VMware vCenter License to the Administration Console....32
Virtual Appliance Management....33
Restarting the Virtual Appliance....33
Updating a Repository Location and Virtual Appliance....33
Updating the Virtual Appliance Software Version....34
Downloading the Troubleshooting Bundle....34
Setting Up The HTTP Proxy....34
Setting Up the NTP Servers....35
Generating a Certificate Signing Request....35
Setting up Global Alerts....36
Managing Backup And Restore....36
Configuring Backup And Restore....36
Scheduling Automatic Backups....37
Performing An Immediate Backup....37
Restoring the Database from a Backup....37
Understanding the vSphere Client Console....38
Configuring Network Settings....38
Changing the Virtual Appliance Password....38
Setting The Local Time Zone....39
Rebooting Virtual Appliance....39
Resetting The Virtual Appliance To Factory Settings....39
Refreshing the Console View....40
Read-only User Role....40
Migration Path to migrate from 1.6/1.7 to 2.0....40
8 About Logs....43
Viewing the Logs....43
Exporting Log Files....44
9 Settings....45
Editing the OMSA Link....45
Understanding Using OMSA with 11th Generation Servers....45
Deploying The OMSA Agent Onto An ESXi System....46
Deploying the OMSA Agent onto an ESX System....46
Setting Up An OMSA Trap Destination....46

10 Viewing Warranty Expiration Notification Settings....49
Configuring Warranty Expiration Notification....49
11 About Firmware Updates....51
Setting Up the Firmware Update Repository....51
Running The Firmware Update Wizard for a Single Host....52
Running the Update Firmware Wizard for a Cluster....53
12 Understanding Events And Alarms....55
Configuring Events And Alarms....56
Viewing Events....57
Viewing the Alarm and Event Settings....57
Viewing the Data Retrieval Schedules for Inventory and Warranty....57
13 Monitoring a Single Host....59
Viewing Host Summary Details....59
Launching Management Consoles....61
Launching the Remote Access Console (iDRAC)....62
Setting Up Physical Server Blink Indicator Light....62
14 Buying and Uploading a Software License....63
About OpenManage Integration for VMware vCenter Licensing....63
15 Viewing Hardware: FRU Details for a Single Host....65
16 Viewing Hardware: Processor Details for a Single Host....67
17 Viewing Hardware: Power Supply Details for a Single Host....69
18 Viewing Hardware: Memory Details for a Single Host....71
19 View Hardware: NICs Details for a Single Host....73
20 Viewing Hardware: PCI Slots for a Single Host....75
21 Viewing Hardware: Remote Access Card Details for a Single Host....77
22 Viewing Storage Details for a Single Host....79
Viewing Storage: Virtual Disk Details for a Single Host....79
Viewing Storage: Physical Disk Details for a Single Host....80
Viewing Storage: Controller Details for a Single Host....81
Viewing Storage: Enclosure Details for a Single Host....82

23 Viewing Firmware Details for a Single Host....83
24 Viewing Power Monitoring for a Single Host....85
25 Viewing Warranty Status for a Single Host....87
Renewing Host Warranty....88
26 Quickly Viewing Only Dell Hosts....89
27 Monitoring Hosts on Clusters and Datacenters....91
28 Viewing Overview Details for Datacenters and Clusters....93
29 Viewing Hardware: FRUs for Datacenters or Clusters....95
30 Viewing Hardware: Processor Details for Datacenters or Clusters....97
31 Viewing Hardware: Power Supply Details for Datacenters and Clusters....99
32 Viewing Hardware: Memory Details for Datacenters and Clusters....101
33 Viewing Hardware: NICs Details for Datacenters and Clusters....103
34 Viewing Hardware: PCI Slot Details for Datacenters and Clusters....105
35 Viewing Hardware: Remote Access Card Details....107
36 Viewing Storage: Physical Disks for Datacenters and Clusters....109
37 Viewing Storage: Virtual Disk Details for Datacenters and Clusters....111
38 Viewing Firmware Details for Datacenters and Clusters....113
39 Viewing Warranty Summary Details for Datacenters and Clusters....115
40 Viewing Power Monitoring for Datacenters and Clusters....117
41 Troubleshooting....119
Frequently Asked Questions (FAQ)....119
'Settings' page fails to load, if we navigate away and go back to 'Settings' page....119
Why is the DNS configuration settings restored to original settings after appliance reboot if using DHCP for appliance IP and DNS settings overwritten....119

Using OpenManage Integration for VMware vCenter to update an Intel Network card with the firmware version of 13.5.2 is not supported..... 119
On trying a firmware update with an invalid DUP, the hardware update job status on the vCenter console neither fails nor times-out for hours, though the job status in LC says 'FAILED'. Why is this happening?.....120
Administration Portal is still showing the unreachable Update Repository location.....120
Why do I see "Task cannot be scheduled for the time in the past" error in inventory schedule/ Warranty schedule page of Initial Configuration Wizard.....120
Why did my system not enter maintenance mode when I performed a one-to-many firmware update?..... 120
Warranty and Inventory schedule for all Vcenters is not applying when selected under "Dell Home > Monitor > Job Queue > Warranty/Inventory History >Schedule"..... 120
Why is the Installation date showing up as 12/31/1969 for some of the firmware on the firmware page.....121
Why is successive Global refresh cause exception to be thrown in Recent Task window..... 121
Why is the Web client UI distorted for few of the Dell screens in IE 10..... 121
Even if my repository has bundles for selected 11G system, why is firmware update showing that I have no bundles for Firmware Update?..... 121
Why am I not seeing the OpenManage Integration Icon on the Web Client even if the registration of the plug-in to the vCenter was successful?.....121
I get an exception whenever I click finish after editing a connection profile through Web Client. Why?.... 122
I am unable to see the connection profiles to which a host belongs to when I create\edit a connection profile in web GUI. Why?.....122
On editing a Connection profile the select host window in the Web UI is blank. Why?..... 122
How Come I See An Error Message Displayed After Clicking The Firmware Link?.....122
What generation of Dell servers does the OpenManage Integration for VMware vCenter configure and support for SNMP traps?..... 123
What vCenters in linked mode are managed by OpenManage Integration for VMware vCenter?..... 123
Does OpenManage Integration for VMware vCenter support vCenter in linked mode?..... 123
What are the Required Port Settings for the OpenManage Integration for VMware vCenter?..... 123
What are the Minimum requirements for successful installation and operation of the virtual appliance?.. 125
How Do I Find the Expected Translations for Renewing Warranty?.....125
How come I do not see my new iDRAC version details listed on the vCenter Hosts & Clusters page?..... 125
How Do I Test Event Settings by Using OMSA to Simulate a Temperature Hardware Fault?..... 126
I Have the OMSA Agent Installed on a Dell Host System, But I Still Get an Error Message That OMSA is Not Installed. What Should I Do?..... 126
Can the OpenManage Integration for VMware vCenter Support ESX/ESXI with Lockdown Mode Enabled?.....126
Inventory is Failing on Hosts ESXi 4.0 Update2 and ESXi Update 3 in Lockdown Mode after a Reboot..... 127
When I tried to use lockdown mode, it failed.....127
What Setting Should I Use For UserVars.CIMoeMProviderEnable With ESXi 4.1 U1?..... 127
I Am Using A Reference Server to Create a Hardware Profile But it Failed. What Should I Do?..... 127
I Am Attempting to Deploy ESX/ESXi on a Blade Server and it Failed. What Should I Do?..... 127
Why are My Hypervisor Deployments Failing on my Dell PowerEdge R210 II Machines?..... 128

Why Do I See Auto-discovered Systems Without Model Information in the Deployment Wizard..... 128
The NFS Share is Set Up With the ESX/ESXI ISO, but Deployment Fails with Errors Mounting the Share Location..... 128
How Do I Force Removal of the Virtual Appliance?..... 128
Entering a Password in the Backup Now Screen Receives an Error Message..... 128
In the vSphere Web Client, Clicking the Dell Server Management Portlet Or the Dell Icon Returns A 404 Error..... 128
My Firmware Update Failed. What Do I Do?..... 129
My vCenter Registration Failed. What Can I Do?..... 129
Performance during Connection Profile Test Credentials is extremely slow or unresponsive..... 129
Does the OpenManage Integration for VMware vCenter support the VMware vCenter Server appliance?..... 129
Does the OpenManage Integration for VMware vCenter support the vSphere Web Client?..... 129
Bare Metal Deployment Issues..... 129
Contacting Dell..... 130
Where To Get Additional Help For This Software..... 130
OpenManage Integration for VMware vCenter Related Information..... 130

42 Virtualization—Related Events..... 131

A Security Roles and Permissions..... 136

A Data Integrity..... 137

A Access Control Authentication, Authorization, and Roles..... 138

A Dell Operation Role..... 139

A Dell Infrastructure Deployment Role..... 140

A Understanding Privileges..... 141

B Understanding Auto-Discovery..... 143
Auto-Discovery Prerequisites..... 143
Enabling or Disabling Administrative Accounts on iDRAC Servers..... 144
Manually Configuring a PowerEdge 11th Generation Server for Auto-Discovery..... 144
Manually Configuring a PowerEdge 12th Generation Server for Auto-Discovery..... 146

1 Introduction

VMware vCenter is the primary console used by IT administrators to manage and monitor VMware vSphere ESX/ESXi hosts. In a standard virtualized environment, VMware alerts and monitoring are used to prompt you to launch a separate console to resolve hardware issues. OpenManage Integration for VMware vCenter is a product that lets you manage VMware vCenter servers from within the VMware Web client, freeing you from being tied to a Windows system. Using OpenManage Integration for VMware vCenter, you have capabilities to manage and monitor Dell hardware within the virtualized environment, such as:

- Alerts and environmental monitoring: Detect key hardware faults and perform virtualization-aware actions (for example, migrate workloads or place host in maintenance mode).
- Single server monitoring and reporting: Monitoring and reporting capabilities of servers.
- Firmware updates: Update Dell hardware to the most recent version of BIOS and firmware.
- Enhanced deployment options: Create hardware profiles, hypervisor profiles, and deploy any combination of the two on bare-metal Dell PowerEdge servers, remotely and without PXE—using vCenter

OpenManage Integration for VMware vCenter Features

You can use the OpenManage Integration for VMware vCenter to perform:

Inventory	Inventory key assets, perform configuration tasks, and provide cluster and datacenter views of Dell platforms.
Monitoring and Alerting	Detect key hardware faults and perform virtualization-aware actions (for example, migrate workloads or place host in maintenance mode). Provide additional intelligence (inventory, events, alarms) to diagnose server problems. Report at the datacenter and cluster view and export to CSV file.
Firmware Updates	Update Dell hardware to the most recent version of BIOS and firmware.
Deployment and Provisioning	Create hardware profiles, hypervisor profiles, and deploy any combination of the two on bare-metal Dell PowerEdge servers, remotely and without PXE—using vCenter.
Service Information	Retrieve warranty information from Dell online.
Security Role and Permissions	Integrate with standard vCenter authentication, rules, and permissions.

2

Understanding How to Configure or Edit the OpenManage Integration for VMware vCenter

After you complete the basic installation of the OpenManage Integration for VMware vCenter, the Initial Configuration Wizard is displayed when you click on the Dell Icon. Use the Initial Configuration Wizard to configure the Settings on first launch. For subsequent instances use the **Settings** page. Also, from the Initial Configuration Wizard you can edit the settings of warranty, inventory, events and alarms. Although using the Initial Configuration Wizard is the most common method used, you can also accomplish this task through the appliance's **OpenManage Integration** → **Manage** → **Settings** page in the OpenManage Integration for VMware vCenter. For more information on the Initial Configuration Wizard, see, **OpenManage Integration for VMWare vCenter User Guide.**

Configuration Tasks Using the Configuration Wizard

The Initial Configuration Wizard can be used to configure the following for one vCenter or for all registered vCenters:

1. vCenter Selection
2. Creating A New Connection Profile
3. Scheduling Inventory Jobs
4. Scheduling a Warranty Jobs
5. Configuring Events And Alarms

NOTE: You can also launch the Initial Configuration Wizard using the link **Start Initial Configuration Wizard** under **Basic Tasks** in the **Getting Started** page.

Configuration Wizard Welcome Page

After you install the OpenManage Integration for VMware vCenter, it must be configured.

1. In the **vSphere Web Client**, click on **Home**, and then **OpenManage Integration** Icon
2. The first time you click on the **OpenManage Integration** icon, it opens the **Configuration Wizard**. You can also access this wizard on the **OpenManage Integration** → **Getting Started** → **Start Initial Configuration Wizard** page.

vCenter Selection

The vCenter selection page allows you to select a specific vCenter to configure settings for, or allows you to select all vCenters to configure them.

1. In the **Initial Configuration Wizard**, click on **Next** in the **Welcome** screen.
2. Select one vCenter or all vCenters from the **vCenters** drop-down list. Select an individual vCenter for those not configured yet or if you have added a new vCenter to your environment. The vCenter selection page allows you to select one or more vCenters to configure settings
3. Click **Next** to proceed to the Connection Profile description page.

Creating A New Connection Profile using the Initial Configuration Wizard

A connection profile stores the credentials that the virtual appliance uses to communicate with Dell servers. Each Dell server must be associated with a connection profile to be managed by the OpenManage Integration for VMware vCenter. You may assign multiple servers to a single connection profile. Creating the Connection Profile is similar between the Configuration Wizard and from the OpenManage Integration for VMware vCenter, Settings option.

Prior to using the Active Directory credentials with a connection profile, the Active Directory user account must exist in Active Directory and this account must already be enabled in iDRAC. This wizard is not for creating Active Directory accounts or enabling Active Directory on iDRAC.

NOTE: You are not allowed to create a connection profile if the number of hosts added exceeds the license limit for Creating a Connection Profile

To create a new connection profile using the wizard:

1. From the **Connection Profile Description** page, Click **Next** to proceed.
2. In the **Name and Credentials** page, enter the **Connection Profile Name** and an optional **Connection Profile Description**
3. In the **Name and Credentials** page, under Credentials, do one of the following:

   NOTE: The iDRAC account requires administrative privileges for updating firmware, applying hardware profiles, and deploying hypervisor.

   – For iDRACs already configured and enabled for Active Directory on which you want to use Active Directory, select the **Use Active Directory** check box; otherwise skip down to configure the iDRAC credentials.

   * In the **Active Directory User Name** text box, type the user name. Type the username in one of these formats: domain\username or username@domain. The user name is limited to 256 characters. Refer to Microsoft Active Directory documentation for user name restrictions.
   * In the **Active Directory Password** text box, type the password. The password is limited to 127 characters.
   * In the **Verify Password** text box, type the password again.
   * In the Certificate Check box, select one of the following:

     • To download and store the iDRAC certificate and validate it during all future connections, select **Enabled** .

     • To perform no check and not store the certificate, do not select the **Enable Certificate Check** check box.

     • For iDRACs already configured and enabled for Active Directory on which you want to use Active Directory, select the **Use Active Directory** check box; otherwise skip down to configure the iDRAC credentials.

   – To configure iDRAC credentials without Active Directory, do the following:

   * In the **User Name** text box, type the user name. The user name is limited to 16 characters. Refer to the iDRAC documentation for information about user name restrictions for your version of iDRAC.

     NOTE: The local iDRAC account requires administrative privileges for updating firmware, applying hardware profiles, and deploying hypervisor.
   * In the **Password** text box type the password. The password is limited to 20 characters.

* In the **Verify Password** text box, type the password again.
* In the Certificate Check box, select one of the following:
    - To download and store the iDRAC certificate and validate it during all future connections, select **Enabled**.
    - To perform no check and not store the iDRAC certificate, do not select the **Enable Certificate Check** check box.

4. In the Host Root area, do one of the following:
   – For hosts already configured and enabled for Active Directory on which you want to use Active Directory, select the **Use Active Directory** check box; otherwise skip down to configure your Host Credentials.
     * In the **Active Directory User Name** text box, type the user name. Type the username in one of these formats: domain\username or username@domain. The user name is limited to 256 characters. Refer to Microsoft Active Directory documentation for user name restrictions.
     * In the **Active Directory Password** text box, type the password. The password is limited to 127 characters.
     * In the **Verify Password** text box, type the password again.
     * In the Certificate Check box, select one of the following:
       - To download and store the Host certificate and validate it during all future connections, select **Enabled**.
       - To perform no check and not store the Host certificate, select **Disabled**.
   – To configure Host Credentials without Active Directory, do the following:
     * In the **User Name** text box, the user name is root. This is the default username and you cannot change the username. but, if the Activate directory is set, you can choose any Active directory user not just root.
     * In the **Password** text box type the password. The password is limited to 127 characters.

       NOTE: The OMSA credentials are the same credentials used for ESX and ESXi hosts.
     * In the **Verify Password** text box, type the password again.
     * In the **Certificate Check** check box, select one of the following:
       - To download and store the Host certificate and validate it during all future connections, select **Enabled** .
       - To perform no check and not store the Host certificate, do not select the **Enable Certificate Check** check box.
5. Click **Next**.
6. In the **Associated Hosts** page, select the hosts for the connection profile and click **OK**.
7. To test the connection profile, select one or more hosts and select the **Test Connection** button. This step is optional. This is used to check whether the Host and iDRAC credentials are correct or not.
8. To complete the profile, click **Next**. For servers that do not have either an iDRAC Express or Enterprise card, the iDRAC test connection result states Not Applicable for this system.

Scheduling Inventory Jobs [Wizard]

The inventory schedule configuration is similar between the Configuration Wizard and from the OpenManage Integration under Manage section, Settings option.

NOTE: To make sure that the OpenManage Integration for VMware vCenter continues to display updated information, it is recommended that you schedule a periodic inventory job. The inventory job consumes minimal resources and will not degrade host performance.

To schedule an inventory job:

1. In the **Configuration Wizard**, in the **Inventory Schedule** window, do one of the following:
   - The **Enable Inventory Data Retrieval** check box is selected by default to enable you to schedule the inventory.
2. Under **Inventory Data Retrieval Schedule**, do the following:
   a) Select the check box next to each day of the week that you want to run the inventory. By default, **all the days** are selected.
   b) In the text box, enter the time in HH:MM format.
   The time you enter is your local time. Calculate the time difference you need to run the inventory collection at the proper time.
3. To apply the changes and continue, click **Next** to proceed with the warranty schedule settings.

Running A Warranty Retrieval Job [Wizard]

The warranty retrieval job configuration is similar between the wizard and from the Dell OpenManage Integration for VMware vCenter, Settings option. In addition, you can run the Warranty Retrieval Job now, from Job Queue. Scheduled jobs would be listed in the Job queue.

To run a warranty retrieval job:

1. In the **Configuration Wizard**, in the **Warranty Schedule** window, do one of the following:
   - Select the **Enable Warranty Data Retrieval** check box to enable you to schedule the warranty.
2. Under **Warranty Data Retrieval Schedule**, do the following:
   a) Select the check box next to each day of the week that you want to run the warranty.
   b) In the text box, enter the time in HH:MM format.
   The time you enter is your local time. Calculate the time difference you need to run the warranty collection at the proper time.
3. To apply the changes and continue, click **Next** to proceed with the warranty schedule settings.

Configuring Events And Alarms [Wizard]

Configure events and alarms using the Configuration Wizard or from the Dell OpenManage Integration for VMware vCenter, Settings option for Events and Alarms.

NOTE: On hosts prior to Dell PowerEdge 12th generation servers, this feature requires that the virtual appliance IP address is configured in the trap destination list in OMSA to display host events in vCenter.

To configure events and alarms:

1. In the **Initial Configuration Wizard**, under **Event Posting Levels**, select one of the following:
   - Do not post any events - Block hardware events.
   - Post All Events - Post all hardware events.
   - Post only Critical and Warning Events - Post only critical or warning level hardware events.

– Post only Virtualization-Related Critical and Warning Events - Post only virtualization-related critical and warning events; this is the default event posting level.

2. To enable all hardware alarms and events, select the **Enable Alarms for Dell Hosts** check box.

   NOTE: Dell hosts that have alarms enabled respond to critical events by entering maintenance mode.

3. A dialog box **Enabling Dell Alarm Warning** is displayed, click **Continue** to accept the change, or click **Cancel**. You should click on **Continue** for the clusters displayed when the DRS is not enabled.

   NOTE: This step is only seen if **Enable Alarms For Dell Hosts** is selected.

4. To continue the wizard, click **Apply**.

3

About VMware vCenter Web Client Navigation

Navigating around VMware vCenter is easy. When you log in to VMware vCenter and land on the home page and Home Tab, the OpenManage Integration icon is located in the main content area under the Administration group. Use the OpenManage Integration icon to locate the OpenManage Integration for VMware vCenter tab and to locate the Dell group in the Navigator area.

VMware vCenter layout has the following three main sections:

Navigator	The Navigator area is the primary menu used to access the different views in the console. OpenManage Integration for VMware vCenter has a special group under the vCenter menu that serves as the primary access point for OpenManage Integration for VMware vCenter.
Main Content area	Displays the views selected in the Navigator. The main content area is the area where most of the content displays.
Notifications	Displays vCenter alarms, task and work in progress. OpenManage Integration for VMware vCenter integrates with the alarm, event and task systems in vCenter to display its own information in the Notification area.

Navigating to the OpenManage Integration for VMware vCenter Inside the VMware vCenter

The OpenManage Integration for VMware vCenter is located in a special Dell group within VMware vCenter.

1. Log in to VMware vCenter.
2. In VMware vCenter home page, click the OpenManage Integration icon.

   From here you can manage OpenManage Integration for VMware vCenter connection profiles, product settings, monitor inventory and warranty jobs, view the summary page and much more from the tabs in the main content area.
3. To monitor hosts, datacenters, and clusters, in the left-side Navigator, under Inventory Lists, select the host, datacenter or cluster you want to investigate and then on the Object tab, click the object you want.
4. Use the Summary or Monitor tab to help you monitor activities or tasks from other Dell hosts.

Understanding Icon Buttons

The product user interface uses many icon-based action buttons for the actions you take.

Table 1. Icon buttons defined.

Icon Button	Definition
	Use this plus-sign icon to add or create something new.
	Use this add server icon to add a server to a connection profile, datacenter, and cluster,

Icon Button	Definition
	Use this icon to abort a job.
	Use this icon to collapse a list.
	Use this icon to expand a list.
	Use this icon to delete an object.
	Use this icon to change a schedule.
	Use this pencil icon to edit.
	Use this broom icon to purge a job.
	Use this icon to export a file.

Locating the Software Version

The software version is found on the OpenManage Integration for VMware vCenter Getting Started tab.

1. In VMware vCenter home page, click the OpenManage Integration icon.
2. On the OpenManage Integration for VMware vCenter Getting Started tab, click **Version Information**.
3. On the Version Information dialog box, view the version information.
4. To close the dialog box, click **OK**.

Refreshing the Screen Content

Refresh the screen at anytime using the VMware vCenter Refresh icon.

1. Select a page that you want to refresh.
2. In the VMware vCenter title bar, click the **Refresh** button.
   The Refresh icon is left of the Search area and looks like a clockwise arrow.

Viewing the OpenManage Integration for VMware vCenter Licensing Tab

When you install OpenManage Integration for VMware vCenter license, the number of supported hosts and vCenters is displayed on this tab. You can also view the version of the OpenManage Integration for VMware vCenter at the top of the page. This page under **License Management** has links to:

- Product Licensing Portal (Digital Locker)
- iDRAC Licensing Portal
- Administration Console

In the OpenManage Integration for VMware vCenter, on the Licensing tab, view the following:

	Licensing
Host Licenses	– Licenses Available Displays the number of available licenses. – Licenses In Use Displays the number of licenses in use.
vCenter Licenses	– Licenses Available Displays the number of available licenses. – Licenses In Use Displays the number of licenses in use.

Opening Online Help

You can open the online help from the Help and Support tab. You can search the document for help on understanding a topic or for a procedure. Online Help contains most of the product User's Guide.

1. In OpenManage Integration for VMware vCenter. Do one of the following:
   - In the Help and Support, under Product Help, click **OpenManage Integration for VMware vCenter Online Help**.
2. Use the left-pane table of contents or search to find the topic of your choice.
3. When finished with Help, in the upper right-hand corner, click the **red X**.

Finding Help and Support

To provide you with the information you need about your product, OpenManage Integration for VMware vCenter offers the Help and Support tab. On this tab, you can find the following information:

Product Help	Provides the following links: • OpenManage Integration for VMware vCenter Help Provides a link to the product help, which is located inside the product. Use the table of contents or search to find the help you need. • About This link brings up the Version Information dialog box. You can find the product version here.
Dell Manuals	Provides live links to: • Server Manuals • OpenManage Integration for VMware vCenter Manuals
Administration Console	Provides a link to the Administration Console.
Additional Help and Support	Provides live links to: • iDRAC with Lifecycle Controller Manuals • Dell VMware Documentation

- OpenManage Integration for VMware vCenter Product Page
- Dell Help and Support Home
- Dell TechCenter

Support Call Tips	Offers tips on how to contact Dell Support and route your calls correctly.
Troubleshooting Bundle	Download a troubleshooting bundle. Provide or refer to this bundle when you contact technical support. For more information, see **Download a Troubleshooting Bundle**
Dell Recommends	Dell recommends Dell Repository Manager and you can find a link to it here. Use Dell Repository Manager to find and download all firmware updates available for your system.
iDRAC Reset	Provides a Reset iDRAC button to use when iDRAC is not responsive. This reset performs a normal iDRAC reboot. See **Resetting iDRAC**

1. In the OpenManage Integration for VMware vCenter, click the **Help and Support** tab.
2. View the OpenManage Integration for VMware vCenter support information on this tab.

4

Connection Profiles

The Connection Profiles tab lets you manage and configure connection profiles. A connection profile stores the credentials that the virtual appliance uses to communicate with Dell servers. Associate each Dell server with only one connection profile for management by the OpenManage Integration for VMware vCenter. You may assign multiple servers to a single connection profile.

- Viewing Connection Profiles
- Creating a Connection Profile
- Editing a Connection Profile
- Refreshing a Connection Profile
- Deleting a Connection Profile
- Testing a Connection Profile

Viewing Connection Profiles

Create a connection profile before you can view it.

Once you have created a connection profile, view it here on the Connection Profile page. The OpenManage Integration for VMware vCenter uses connection profiles to communicate with Dell hosts.

In OpenManage Integration for VMware vCenter, on the **Manage** → **Connection Profile tab** , you can view all the connection profiles you have created. The information you can view includes:

Profile Name	Displays the name of the connection profile.
Description	Displays a description, if provided.
vCenter	Displays the IP address of the vCenter.
Associated Hosts	Displays the hosts associated with this connection profile. If more than one, use the expand icon to show all.
iDRAC Certificate Check	Shows whether the iDRAC Certificate Check is enabled or disabled.
Host Root Certificate Check	Shows whether the Host Root Certificate Check is enabled or disabled.
Date Created	Displays the create date.
Date Modified	Displays the Modify date.
Last Modified By	Displays who last modify this profile.

Creating A Connection Profile

You may assign multiple servers to a single connection profile. Create a Connection Profile using the OpenManage Integration for VMware vCenter**Manage** → **Connection Profiles** tab and click the Plus sign to proceed.

NOTE: The vCenter hosts that display during this procedure have authenticated using the same Single Sign On (SSO). If you do not see a vCenter host, it may be on a different SSO or you may be using a VMware vCenter version less than version 5.1.

1. In the OpenManage Integration for VMware vCenter, on the **Manage** → **Connection Profiles** tab, click the **Create New** icon.
2. In the **Connection Profile Description** page, click **Next**.
3. In the **Name and Credentials** page, do the following:
   a) Under Profile, type the **Profile Name** and optional **Description**.
   b) Under vCenter, select the host or hosts on which you want to associate with this connection profile. This option lets you create one connection profile for many vCenter hosts.
   c) Under **Name and Credentials** page, do the following:
      * The iDRAC account requires administrative privileges for updating firmware, applying hardware profiles, and deploying hypervisor.
      * In the **Active Directory User Name** text box, type the user name. Type the username in one of these formats: domain\username or username@domain. The user name is limited to 256 characters. Refer to Microsoft Active Directory documentation for user name restrictions.
      * In the **Active Directory Password** text box, type the password. The password is limited to 127 characters.
      * In the **Verify Password** text box, type the password again
      * In the Certificate Check box, select one of the following:
      * To download and store the iDRAC certificate and validate it during all future connections, select **Enabled**.
      * To perform no check and not store the certificate, do not select the **Enable Certificate Check** check box.
   d) In the **Hosts Root** page, do the following:.
      * For hosts already configured and enabled for Active Directory on which you want to use Active Directory, select the **Use Active Directory** check box; otherwise skip down to configure your Host Credentials.
      * In the **Active Directory User Name** text box, type the user name. Type the username in one of these formats: domain\username or username@domain. The user name is limited to 256 characters. Refer to Microsoft Active Directory documentation for user name restrictions.
      * In the **Active Directory Password** text box, type the password. The password is limited to 127 characters.
      * In the **Verify Password** text box, type the password again.
      * In the Certificate Check box, select one of the following:
      * To download and store the Host certificate and validate it during all future connections, select **Enabled**.
      * To perform no check and not store the Host certificate, select **Disabled**.
      * To configure Host Credentials without Active Directory, do the following:
      * In the **User Name** text box, the user name is root. This is the default username and you cannot change the username
      * If the Activate directory is set, you can choose any Active directory user not just root.
      * In the **Password** text box type the password. The password is limited to 127 characters.

NOTE: The OMSA credentials are the same credentials as those used for ESX and ESXi hosts.

* In the **Verify Password** text box, type the password again.
* In the **Certificate Check** check box, select one of the following:
* To download and store the Host certificate and validate it during all future connections, select **Enabled**
* To perform no check and not store the Host certificate, do not select the **Enable Certificate Check** check box.

4. Click **Next**.
5. In the Associated Hosts page, select the hosts for the connection profile and click **OK**.
6. To test the connection profile, select one or more hosts and select the Test Connection button. This step is optional. This is used to check whether the Host and iDRAC credentials are correct or not.
7. To complete the profile, click **Next**. For servers that do not have either an iDRAC Express or Enterprise card, the iDRAC test connection result states Not Applicable for this system.

Editing a Connection Profile

After you have configured a connection profile, you can edit the profile name, description, associated hosts, and credentials.

NOTE: The vCenters that display during this procedure have authenticated using the same Single Sign On (SSO). If you do not see a vCenter host, it may be on a different SSO or you may be using a VMware vCenter version less than version 5.1.

NOTE: You are not allowed to edit a connection profile if the number of hosts added exceeds the license limit.

1. In the OpenManage Integration for VMware vCenter, on the **Manage → Connection Profiles** tab, select a connection profile.
2. Click the **Edit** icon.
3. In the Connection Profile window, on the Welcome tab, read the information and click **Next**.
4. In the Name and Credentials tab, do the following:
   a) Under Profile, type the **Profile Name** and optional **Description**.
   b) Under vCenter, view the associated hosts for this connection profile. See the note above about why you see the hosts displayed here.
   c) Under iDRAC Credentials, do the following:

      * The user name is root and this entry cannot be modified if you do not select the **Active Directory**. If the **Activate directory** is set, you can choose any Active directory user not just root.
      * Domain\Username: Type the username in one of these formats: domain\username, or domain@username.

        NOTE: The following characters are allowed for the user name: / (forward slash), &, \ (backslash), . (period), " (quotation mark), @, % (percent) (127 character limit).

        The domain can contain alphanumeric characters and -
        (dash) and . (period) only (254 character limit). The first and last characters for domain must be alphanu meric.
      * Password: Type your password.

        The following characters are not allowed for the password: / (forward slash), &, \ (backslash), . (period), " (quotation mark).
      * Verified password: Type your password again.

* Enable Certificate Check: The default is a cleared check box. To download and store the iDRAC certificate and validate it during all future connections, select **Enable Certificate Check**, or clear the **Enable Certificate Check** check box to perform no certificate check and not store the certificate.

  NOTE: You need to select **Enable** if you are using Active-Directory.

d) Under Host Root, do the following:

* Select the **Use Active Directory** check box to access all the consoles associated with the active directory.

  Username: The default usertname is **root** and cannot be modified. If the Use Active Directory is selected, you can use any active directory user name.

* Password: Type your password.

  The following characters are not allowed for the password: / (forward slash), &, \ (backslash), . (period), " (quotation mark).

* Verified password: Type your password again.

* Enable Certificate Check: The default is a cleared check box. To download and store the iDRAC certificate and validate it during all future connections, select **Enable Certificate Check**, or clear the **Enable Certificate Check** check box to perform no certificate check and not store the certificate.

  NOTE: You need to select **Enable** if you are using Active-Directory.

NOTE: The OMSA credentials are the same credentials as those used for ESX and ESXi hosts.

NOTE: For servers that do not have either an iDRAC Express or Enterprise card, the iDRAC test connection result states *Not Applicable for this system*.

5. Click **Next**.
6. In the Select Hosts dialog box, select the hosts for this connection profile.
7. Click **OK**.
8. The Associated Host tab lets you test the iDRAC and Host Credentials on the selected servers. Do one of the following:

   – To begin the test, select the hosts to check and then click the **Test Connection** icon. The other options are inactive.

     When the test is done click **Finish**.

   – To stop the tests click **Abort All Tests**. In the Abort Tests dialog box, click **OK**, and then click **Finish**.

Refreshing A Connection Profile

In the OpenManage Integration for VMware vCenter, on the **Manage** → **Connection Profiles** tab, up in the VMware vSphere Web Client title bar, click the **Refresh** icon.

NOTE: After removing the host from vCenter, when you navigate to connection profile page, you will be prompted to remove the host from connection profile. Upon confirmation, the host will be removed from Connection Profile.

Deleting A Connection Profile

1. In the OpenManage Integration for VMware vCenter, on the **Manage** → **Connection Profiles** tab, select the profiles to delete.
2. Click the **Delete** icon.

3. On the Delete Confirmation message, to remove the profile, click **Yes** , or click **No** to cancel the delete action.

Testing a Connection Profile

1. In the OpenManage Integration for VMware vCenter, on the **Manage** → **Connection Profiles** tab, select a connection profile to test. This action may take several minutes to complete.
2. In the Test Connection Profile dialog, select the hosts you want to test and then click the **Test Connection** icon.
3. To abort all selected tests and cancel the testing, click **Abort All Tests**. In the Abort Tests dialog box, click **OK**.
4. To exit, click **Cancel**.

5

Inventory History

Inventory Jobs are set up using the Settings tab or the Initial Configuration wizard. Use the Inventory History tab to view your inventory jobs. Tasks you can do from this tab include:

- Viewing Inventory History
- Changing Inventory Job Schedules
- Running an Inventory Job Now

Viewing Inventory History

A successful completed inventory is required to gather the data. Once the inventory is complete, you can view the inventory results for the entire datacenter or for an individual host system. See Running an Inventory Job Now. Columns are sortable in ascending and descending order.

If server data cannot be retrieved and displayed, there are several possible causes:

- The server is not associated with a connection profile, and therefore you cannot run an inventory job.
- An inventory job has not been run on the server to collect the data, and therefore there is nothing to display.
- The number of host licenses is exceeded, and you must have additional licenses available for the inventory task to complete.
- The server does not have the correct iDRAC license required for Dell PowerEdge 12th generation servers and you must purchase the correct iDRAC licence.

1. In the OpenManage Integration for VMware vCenter, click the **Monitor** tab.
2. Click **Job Queue** → **Inventory History.**
3. To view the server information on a selected vCenter, select a vCenter to display all associated host details.
4. Review the Inventory History information.

	vCenter Details
Change Schedule button	Click to edit an inventory schedule.
Run Now button	Click to run an inventory.
vCenter	Displays vCenter Address.
Hosts Passed	Displays any hosts, which have passed.
Next Inventory	Displays the next inventory schedule that will run.
Last Inventory	Displays the last inventory schedule that was run.
	Hosts
Host	Displays the host address.
Status	Displays the status. Options include:

	– Successful – Failed – In Progress – Scheduled
Duration (MM:SS)	Displays the duration of the job in minutes and seconds.
Start Date and Time	Displays the date and time when the inventory schedule started.
End Date and Time	Displays the time the inventory schedule ended.

Changing Inventory Job Schedules

To make sure there is up-to-date server information you must run periodic inventories on Dell servers. Dell recommends running an inventory once a week. Inventories do not impact host performance. You can change a inventory job schedule on the **Monitor** → **Job Queue** → **Inventory History** page or from the **Manage** → **Settings** page.

1. In the OpenManage Integration for VMware vCenter, on the **Monitor** → **Job Queue** tab, click **Inventory History**.
2. Select a vCenter and then click the **Change Schedule** icon.
3. In the Inventory Data Retrieval dialog box, do the following:
   a) Under Inventory Data, select the **Enable Inventory Data Retrieval** check box.
   b) Under Inventory Data Retrieval Schedule, select the days of the week for your job.
   c) In the Inventory Data Retrieval Time text boxes, type the local time for this job.
   You may need to calculate the time difference required to run this job at the proper time.
4. Click **Apply** to save the settings, **Clear** to reset the settings, and **Cancel** to abort the operation.

Running an Inventory Job Now

Run an inventory job at least once a week.

1. In the OpenManage Integration for VMware vCenter, on the **Monitor** → **Job Queue** tab, click **Inventory History**.
2. Click the **Run Now** button.
3. In the Success dialog box, click **Close**.
   An inventory job is now in queue. Note that you cannot run an inventory for a single host. An inventory job starts it for all hosts

6

Warranty History

Warranty jobs are set up using the Configuration Wizard. View your warranty job history on this tab. Tasks you can do on this tab include:

- Viewing Warranty History
- Changing a Warranty Job Schedule
- Running a Warranty Job Now

Viewing Warranty History

A warranty job is a scheduled task to get warranty information from support.dell.com on all systems. Columns are sortable in ascending and descending order.

1. In the OpenManage Integration for VMware vCenter, click the **Monitor** tab.
2. Click **Job Queue → Warranty History.**
3. View your warranty job history information

Modify Schedule button	Click to edit a warranty job schedule.
Run Now button	Click to run a warranty job.
	vCenter History
vCenters	Displays lists of vCenters.
Hosts Passed	Displays the number of vCenter Hosts that passed.
Last Warranty	Displays the last warranty job that was run.
Next Warranty	Displays the next warranty job that will run.
	Hosts History
Host	Displays the host address.
Status	Displays the status. Options include: – Successful – Failed – In Progress – Scheduled
Duration (MM:SS)	Displays the duration of the warranty job in MM:SS.
Start Date and Time	Displays the date and time when the warranty job started.
End Date and Time	Displays the time the warranty job ended.

Modifying a Warranty Job Schedule

Hardware warranty information is retrieved from Dell Online and displayed by the OpenManage Integration for VMware vCenter. Server's Service Tag is used to gather warranty information about the server. Warranty jobs are originally configured in the Initial Configuration Wizard. Later, you can modify a warranty job schedule on the **Monitor Tab** → **Job Queue** → **Warranty History** page or from the **Manage Tab** → **Settings** page.

1. In the OpenManage Integration for VMware vCenter, on the **Monitor** → **Job Queue** tab, click **Warranty History**.
2. Click the **Change Schedule** icon.
3. In the Warranty Data Retrieval dialog box, do the following:
   a) Under Warranty Data, select the **Enable Warranty Data Retrieval** check box.
   b) Under Warranty Data Retrieval Schedule, select the days of the week for your job.
   c) In the Warranty Data Retrieval Time text boxes, type the local time for this job.
      You may need to calculate the time difference required to run this job at the proper time.
4. Click **Apply**.

Running a Warranty Job Now

Run an warranty job at least once a week.

1. In the OpenManage Integration for VMware vCenter, on the **Monitor** → **Job Queue** tab, click **Warranty History**.
2. Click the **Run Now** button.
3. In the Success dialog box, click **Close**.
   An warranty job is now in queue.

7

Console Administration

Administration of the OpenManage Integration for VMware vCenter and its virtual environment is achieved by using two additional administration portals:

- Web-based Administration Console
- Console view for an individual server (the appliance virtual machine console).

Through the use of these two portals, global settings for vCenter management, OpenManage Integration for VMware vCenter database backup and restore, and reset/restart actions can be entered and used across all vCenter instances.

Using the Administration Console

From the vCenter Registration window in the Administration Console, you can register a vCenter server, and upload or buy a license. If you are using a demo license, a Buy Software link displays from which you can purchase a full-version license for managing multiple hosts. In this section you can also modify, update, and unregister a server.

Related Tasks:

- Registering a vCenter Server
  - Modifying the Administrator vCenter Login
  - Updating the SSL Certificates for Registered vCenters
  - Uninstalling OpenManage Integration for VMware vCenter from vCenter
- Uploading a OpenManage Integration for VMware vCenter License

Registering a vCenter Server

You can register vCenter servers with the OpenManage Integration for VMware vCenter after the OpenManage Integration for VMware vCenter is installed. OpenManage Integration for VMware vCenter uses the admin user account for vCenter operations.

1. In OpenManage Integration for VMware vCenter, on the Summary tab, use the link to open the Administration Console.
2. In the Login dialog box, type your password.
3. To register a new server, in the left pane, click **VCENTER REGISTRATION**, and then click **Register New vCenter Server**.
4. In the **Register a New vCenter** dialog box, under **vCenter Name** do the following:
   a) In the **vCenter Server IP or Hostname** text box, enter the vCenter IP address or a hostname.
   b) In the **Description** text box, enter an optional description.
5. Under **Admin User Account**, do the following:
   a) In the **Admin User Name** text box, enter the administrator's user name.
   b) In the **Password** text box, enter the password.
   c) In the **Verify Password** text box, enter the password again.

6. Click **Register**.

Modifying The vCenter Administrator Login

1. In OpenManage Integration for VMware vCenter, on the Summary tab, use the link to open the Administration Console.
2. In the Login dialog box, type your password.
3. In the left pane, click **VCENTER REGISTRATION**. The registered vCenters are displayed in a table. To display the **Modify Admin Acct** window, under **Credentials**, click **Modify**.
4. Enter the vCenter Administrator **User Name**, **Password**, and **Verify Password**; the passwords must match.
5. To change the password, click **Apply**, or to cancel the change click **Cancel**.

Updating The SSL Certificates For Registered vCenter Servers

If the SSL certificate is changed on a vCenter server, then use the following steps to import the new certificate for the OpenManage Integration for VMware vCenter. The OpenManage Integration for VMware vCenter uses this certificate to make sure the vCenter server it is talking to is the correct vCenter server and not an impersonator.

OpenManage Integration for VMware vCenter uses the openssl API to create the Certificate Signing Request (CSR) using the RSA encryption standard with a 2048 bit key length. The CSR generated by the OpenManage Integration for VMware vCenter is used to get a digitally signed certificate from a trusted Certification Authority. The OpenManage Integration for VMware vCenter uses the digital certificate to enable SSL on the Web server for secure communication.

1. Launch a browser window and enter the **Administration Console URL** displayed in the **vSphere vCenter Console tab** for the virtual machine you want to configure or use the link from the **Dell Management Console → Settings page**. The URL uses the following format and is case sensitive: **https://<ApplianceIPAddress>**
2. In the left pane, click **VCENTER REGISTRATION**. The registered vCenters are displayed in a table. To update the certificates, click **Update**.

Uninstalling the OpenManage Integration for VMware vCenter From VMware vCenter

To remove the OpenManage Integration for VMware vCenter, it must be unregistered from the vCenter server using the Administration Console.

1. In OpenManage Integration for VMware vCenter, on the Summary tab, use the link to open the Administration Console.
2. In the Login dialog box, type your password.
3. In the **vCenter Registration** page, under the vCenter server table, unregister the OpenManage Integration for VMware vCenter by clicking **Unregister**.

   You may have more than one vCenter, so be sure select the right one.
4. In the **Unregister vCenter** dialog box that asks if you really want to unregister this server, click **Unregister**.

Uploading a OpenManage Integration for VMware vCenter License to the Administration Console

1. In OpenManage Integration for VMware vCenter, on the Summary tab, use the link to open the Administration Console.
2. In the Login dialog box, type your password.
3. In the left pane, click **VCENTER REGISTRATION**. The registered vCenters are displayed in a table. To display the upload license dialog box, click **Upload License**.
4. To navigate to the license file, click the **Browse** button, to navigate to the license file, and then click **Upload**.

NOTE: If the license file is modified or edited in any way, the appliance views it as corrupted and the file will not work. You can add licenses if you need to add more hosts. Follow the process mentioned above to add more licenses.

NOTE: If the number of successfully inventoried 11G and 12G servers equals the number of purchased licenses, you will be blocked from adding 9G or 10G servers to new or existing connection profiles, Edit existing connection profiles by removing few 11G/12G servers and add 10G/9G instead of them. Create a new connection profile for the removed 11G/12G servers.

Virtual Appliance Management

Virtual appliance management contains the OpenManage Integration for VMware vCenter network, version, NTP, and HTTPS information, and lets you:

- Restart the virtual appliance
- Update the virtual appliance and configure an update repository location
- Download a troubleshooting bundle
- Set up NTP servers
- Upload HTTPS certificates

Restarting the Virtual Appliance

Restarting the virtual appliance logs you out from the Administration Console, and the OpenManage Integration for VMware vCenter is unavailable until the virtual appliance and its services are active.

1. In OpenManage Integration for VMware vCenter, on the Summary tab, use the link to open the Administration Console.
2. In the Login dialog box, type your password.
3. In the left pane, click **APPLIANCE MANAGEMENT**.
4. To restart the OpenManage Integration for VMware vCenter, click **Restart the Virtual Appliance**.
5. On the **Restart Virtual Appliance** dialog box, to restart the virtual appliance click **Apply** or click **Cancel** to cancel.

Updating a Repository Location and Virtual Appliance

Perform a backup prior to an update of the virtual appliance to make sure all data is protected. See, Managing Backup and Restore.

1. In OpenManage Integration for VMware vCenter, on the Summary tab, use the link to open the Administration Console.
2. In the Login dialog box, type your password.
3. In the left pane, click **APPLIANCE MANAGEMENT**.
4. Next to Appliance Update, click **Edit**.
5. In the **Appliance Update** window, enter the **Repository Location URL**, and then click **Apply**.

   NOTE: If the update location is on an external network, such as the Dell FTP site, then a proxy must be entered below in the HTTP Proxy area.

Updating the Virtual Appliance Software Version

To prevent data loss, perform an appliance backup prior to beginning the software update.

1. In OpenManage Integration for VMware vCenter, on the Summary tab, use the link to open the Administration Console.
2. In the Login dialog box, type your password.
3. In the left pane, click **Appliance Maintenance**.
4. To update the virtual appliance to the software version listed under **Appliance Update**, click **Update Virtual Appliance**.
5. In the **Update Appliance** dialog box, the current and available versions are listed. To begin the update, click **Update**.
6. The system is locked down and put into maintenance mode. When the update is complete, the Appliance page displays showing the newly installed version.

Downloading the Troubleshooting Bundle

Use this information to assist in troubleshooting issues, or send to Technical Support.

1. Launch a browser window, and enter the **Administration Console URL** displayed in the **vSphere vCenter Console** tab for the virtual machine you want to configure or use the link from **Dell Management Console → Settings** page. The URL uses the following format and is case-insensitive:

   https://<ApplianceIPAddress>
2. In the left pane, click **APPLIANCE MANAGEMENT**.
3. To display the troubleshooting bundle dialog box, click **Generate Troubleshooting Bundle**.
4. To either open or save a zip file that contains the virtual appliance logging information, click the **Download Troubleshooting Bundle** link.
5. To exit, click **Close**.

Setting Up The HTTP Proxy

You can set up the HTTP proxy settings using the Administration Console or the Dell Management Console.

1. In OpenManage Integration for VMware vCenter, on the Summary tab, use the link to open the Administration Console.
2. In the Login dialog box, type your password.
3. In the left pane, click **APPLIANCE MANAGEMENT**.
4. In the **Appliance Management** page, scroll down to the **HTTP Proxy Settings**, and then click **Edit**.
5. In the **Edit** page, do the following:
   a) To enable the use of HTTP Proxy Settings, next to **Use HTTP Proxy Settings**, select **Enable**.
   b) In the **Proxy Server Address** text box, enter the proxy server address.
   c) In the **Proxy Server Port** text box, enter the proxy server port.
   d) To use proxy credentials, next to **Use Proxy Credentials**, select **Yes**.
   e) If you are using credentials, in the **User Name** text box, enter the user name.
   f) In the **Password** text box, type the password.
6. Click **Apply**.

Setting Up the NTP Servers

Use the Network Time Protocol (NTP) to synchronize the virtual appliance clocks to that of a NTP server.

1. In OpenManage Integration for VMware vCenter, on the Summary tab, use the link to open the Administration Console.
2. In the Login dialog box, type your password.
3. In the left pane, click **APPLIANCE MANAGEMENT**.
4. Click **Edit for NTP**.
5. Select the **Enabled** check box. Enter the **host name** or **IP address** for a **Preferred** and **Secondary NTP Server** and click **Apply**.
6. To exit, click **Cancel**.

Generating a Certificate Signing Request

Generating a new Certificate Signing Request prevents certificates that are created with the previously generated CSR from being uploaded to the appliance.

1. In OpenManage Integration for VMware vCenter, on the Summary tab, use the link to open the Administration Console.
2. In the Login dialog box, type your password.
3. In the left pane, click **APPLIANCE MANAGEMENT**.
4. Click **Generate Certificate Signing Request for HTTPS Certificates**. A message displays stating that if a new request is generated, then certificates created using the previous CSR can no longer be uploaded to the appliance. To continue with the request, click **Continue**, or **Cancel** to cancel.
5. Enter the **Common Name**, **Organizational Name**, **Organizational Unit**, **Locality**, **State Name**, **Country** and **Email** for the request. Click **Continue**.
6. Click **Download**, and then save the resulting HTTPS certificate to an accessible location.

Uploading an HTTPS Certificate

You can use HTTPS Certificates for secure communication between the virtual appliance and host systems. To set up this type of secure communication, a certificate signing request must be sent to a certificate authority and then the resulting certificate is uploaded using the Administration Console. There is also a default certificate that is self-signed and can be used for secure communication; this certificate is unique to every installation.

NOTE: You can use either Microsoft Internet Explorer or Firefox to upload certificates.

1. In OpenManage Integration for VMware vCenter, on the Summary tab, use the link to open the Administration Console.
2. In the Login dialog box, type your password.
3. In the left pane, click **APPLIANCE MANAGEMENT**.
4. Click **Upload Certificate for HTTPS Certificates**.
5. In the **Upload Certificates** dialog box, click **OK**.
6. To select the certificate to upload, click **Browse**, and then click **Upload**.
7. If you want to abort the upload, click **Cancel**.

   NOTE: The certificate must use PEM format.

Restoring the Default HTTPS Certificate

1. In OpenManage Integration for VMware vCenter, on the Summary tab, use the link to open the Administration Console.
2. In the Login dialog box, type your password.
3. In the left pane, click **APPLIANCE MANAGEMENT**.
4. Click **Restore Default Certificate for HTTPS Certificates**.
5. In the restore default certificate dialog box, click **Apply**.

Setting up Global Alerts

Alert management lets you enter global settings for how alerts are stored for all vCenter instances.

1. In OpenManage Integration for VMware vCenter, on the Summary tab, use the link to open the Administration Console.
2. In the Login dialog box, type your password.
3. In the left pane, click **ALERT MANAGEMENT**. To enter new vCenter alert settings, click **Edit**.
4. Enter numeric values for the following items:
   - Maximum number of alerts
   - Number of days to retain alerts
   - Timeout for duplicate alerts (seconds)
5. To save your settings, click **Apply**, or click **Cancel** to cancel.

Managing Backup And Restore

Managing backup and restore is accomplished from the Administrative Console. Tasks on this page include:

- Configuring Backup And Restore
- Scheduling Atomatic Backups
- Performing An Immediate Backup
- Restoring The Database From Backup

Configuring Backup And Restore

The backup and restore function backs up the OpenManage Integration for VMware vCenterdatabase to a remote location from which it can be restored at a later date. Profiles, templates, and host information are included in the backup. It is recommended that you schedule automatic backups to guard against data loss. After this procedure, you must configure a backup schedule.

1. In OpenManage Integration for VMware vCenter, on the Summary tab, use the link to open the Administration Console.
2. In the Login dialog box, type your password.
3. In the left pane, click **BACKUP AND RESTORE**.
4. To edit the current backup and restore settings, click **Edit**.
5. In the **Settings and Details** page, do the following:
   a) In the **Backup Location** text box, type the path to the backup files.
   b) In the **User Name** text box, type the user name.

c) In the **Password** text box, type the password.
d) Under **Enter the password used to encrypt backups**, type the encrypted password in the text box.
The encryption password can contain alpha numeric characters and the following special characters: !@#$%*. There is no length restriction.
e) In the **Verify Password** text box, retype the encrypted password.

6. To save these settings, click **Apply**.
7. Configure the backup schedule. For more information see, Scheduling Automatic Backups.

Scheduling Automatic Backups

This is the second part of configuring backup and restore. For detailed information on configuring the backup location and credentials, see Configuring Backup And Restore.

To schedule an automatic backup:

1. In OpenManage Integration for VMware vCenter, on the Summary tab, use the link to open the Administration Console.
2. In the Login dialog box, type your password.
3. In the left pane, click **BACKUP AND RESTORE**.
4. To edit the backup and restore settings, click **Edit Automatic Scheduled Backup** (this makes fields active).
5. To enable the backups, click **Enabled**.
6. Select the check boxes for the days of the week for which you want to run the backup.
7. In the **Time for Backup (24 Hour Time Format, HH:mm)** text box, enter the time in HH:mm format.
The **Next Backup** populates with the date and time of the next scheduled backup.
8. Click **Apply**.

Performing An Immediate Backup

1. In OpenManage Integration for VMware vCenter, on the Summary tab, use the link to open the Administration Console.
2. In the Login dialog box, type your password.
3. In the left pane, click **BACKUP AND RESTORE**.
4. Click **Backup Now**.
5. To use location and encryption password from the Backup settings, in the **Backup Now** dialog box, select that check box.
6. Enter a **Backup Location**, **User Name**, **Password**, and **Encryption Password**.
The encryption password can contain alpha numeric characters and the following special characters: !@#$%*. There is no length restriction.
7. Click **Backup**.

Restoring the Database from a Backup

NOTE: The restore operation causes the virtual appliance to reboot after it has completed.

1. In OpenManage Integration for VMware vCenter, on the Summary tab, use the link to open the Administration Console.
2. In the Login dialog box, type your password.
3. In the left pane, click **BACKUP AND RESTORE** and the current backup and restore settings are displayed.
4. Click **Restore Now**.

5. In the Restore Now dialog box, enter a **File Location (CIFS/NFS Format)**.
6. Enter the **User Name**, **Password**, and **Encryption Password** for the backup file.

   The encryption password can contain alpha numeric characters and the following special characters: !@#$%*. There is no length restriction.
7. To save your changes, click **Apply**.

   The appliance reboots or restarts once Apply is clicked.

Understanding the vSphere Client Console

The Console is found within the vSphere Web Client on a virtual machine. The Console works hand and hand with the Administration Console. The Console provides the ability to:

- Configure network settings
- Change the virtual appliance password
- Set the local timezone
- Reboot the virtual appliance
- Reset the virtual appliance to factory settings
- Refresh Console

Use the arrow keys to navigate up or down. Once you have selected the option you want, press **<ENTER>**. Once you access the console screen, VMware vSphere Client takes control of your cursor. To escape from that control, press **<CTRL> + <ALT>**.

Configuring Network Settings

Changes to the network settings are done in the vSphere Web Client on the Console.

1. In vSphere Web Client, in the Navigator, select **vCenter**.
2. In the Navigator, select the Virtual Machine that you want to manage.
3. Do one of the following:
   - On the Object tab, select **Action** → **Open Console**.
   - Right-click the virtual machine that you selected and select **Open Console**.
4. In the **Console** window, select **Configure Network**, then press **<ENTER>**.
5. Enter the desired network settings under **Edit Devices** or under **Edit DNS** configuration, then click **Save & Quit**. To abort any changes, click **Quit**.

Changing the Virtual Appliance Password

The virtual appliance password is changed in the vSphere Web Client using the Console.

1. In vSphere Web Client, in the Navigator, select **vCenter**.
2. In the Navigator, select the Virtual Machine that you want to manage.
3. Do one of the following:
   - On the Object tab, select **Action** → **Open Console**.
   - Right-click the virtual machine that you selected and select **Open Console**.
4. On the Console, use the arrow keys to select **Change Admin Password** and press **<ENTER>**.

5. Enter the **Current Admin Password** and press **<ENTER>**.

   Admin passwords include one special character, one number, one uppercase, one lowercase, and at least 8 letters.
6. Enter a new password for **Enter new Admin Password** and press **<ENTER>**.
7. Type the new password again in **Please Confirm Admin Password** text box , and then press **<ENTER>**.

Setting The Local Time Zone

To set the local time zone:

1. In vSphere Web Client, in the Navigator, select **vCenter**.
2. In the Navigator, select the Virtual Machine that you want to manage.
3. Do one of the following:
   - On the Object tab, select **Action** → **Open Console**.
   - Right-click the virtual machine that you selected and select **Open Console**.
4. Use the arrow keys to select **Set Time Zone** and press **<ENTER>**.
5. In the **Timezone Selection** window, select the desired time zone and click **OK**. To cancel changes click **Cancel**. The time zone is updated.

Rebooting Virtual Appliance

To reboot the virtual appliance:

1. In vSphere Web Client, in the Navigator, select **vCenter**.
2. In the Navigator, select the Virtual Machine that you want to manage.
3. Do one of the following:
   - On the Object tab, select **Action** → **Open Console**.
   - Right-click the virtual machine that you selected and select **Open Console**.
4. Use the arrow keys to select **Reboot this Virtual Appliance** and press **<ENTER>**.
5. The following message is displayed:

   ```
   If there are any processes running on this appliance they will be
   terminated by this action. Are you sure you wish to do this?
   ```
6. Enter **y** to reboot or **n** to cancel. The appliance is rebooted.

Resetting The Virtual Appliance To Factory Settings

To reset the virtual appliance to factory settings:

1. In vSphere Web Client, in the Navigator, select **vCenter**.
2. In the Navigator, select the Virtual Machine that you want to manage.
3. Do one of the following:
   - On the Object tab, select **Action** → **Open Console**.
   - Right-click the virtual machine that you selected and select **Open Console**.
4. Use the arrow keys to select **Reset this Virtual Appliance to Factory Settings** and press **<ENTER>**.
5. The following notice is displayed:

   ```
   This operation is completely Irreversible if you continue you will
   completely reset *this* appliance to its original settings. All changes you
   ```

```
have made to this appliance will be Lost. Are you sure you wish to Reset
this Appliance to Factory Settings?
```

6. Enter **y** to reset or **n** to cancel. The appliance is reset to the original factory settings.

   NOTE: When the virtual appliance is reset to factory settings, any updates made to the Network Configuration are preserved; these settings are not reset.

Refreshing the Console View

To refresh the Console view, select **Refresh** and press **<ENTER>**.

Read-only User Role

There is an unprivileged user role called read-only with shell access for diagnostic purposes. The read-only user has limited privileges to run the mount. The read-only user's password is set to the same as the admin.

Migration Path to migrate from 1.6/1.7 to 2.0

OpenManage Integration for VMware vCenter version 2.0 is an OVF release only. There is no RPM update path from the older versions to this version. You can migrate from older version (1.6 or 1.7) to the version 2.0 release using the Backup and Restore path. Also, the migration path is only supported from version 1.6 and 1.7. If you are at a lower version than 1.6, you will have to upgrade your appliance to the supported version before you perform the migration to OpenManage Integration for VMware vCenter version 2.0.

Do the following to migrate from older version to the OpenManage Integration for VMware vCenter 2.0 version:

1. Take a Backup of the database for the older release. For more information, See the section, **Managing Backup and Restore** in this guide.
2. Power off the older appliance from the vCenter.

   NOTE:

   Do not unregister the Plug-in from the vCenter. Unregistering the plug-in from the vCenter will remove all the Alarms registered on the vCenter by the plug-in and remove all the customizing performed on the alarms like actions and so on, on the vCenter. For more information, see the section **How to recover if I have unregistered the older plugin after the backup** in this guide if you have already unregistered the Plug-ins after the backup.
3. Deploy the new OpenManage Integration version 2.0 OVF. For more information, see the section **Deploying the OpenManage Integration for VMware vCenter OVF Using the vSphere Client** in this guide to deploy the OVF.
4. Power on the OpenManage Integration version 2.0 appliance.
5. Setup the network, time zone and so on to the appliance. It is recommended that the new OpenManage Integration version 2.0 appliance has the same IP address as the old appliance. To setup the network details, see the section, **Registering OpenManage Integration for VMware vCenter And Importing The License File** in this guide.
6. Restore the database to the new appliance. For more information, see the section, **Restoring The Database From A Backup** in this guide.
7. Upload the new license file. For more information, see the section, **Registering OpenManage Integration for VMware vCenter And Importing The License File** in **OpenManage Integration Version 2.0 Quick Install Guide**.
8. Verify the appliance. For more information, see the section **Installation Verification** in this guide to ensure the database migration is successful.
9. Run the Inventory on all the registered vCenters.

NOTE:

It is recommended that you run the inventory on all the hosts managed by the plug-in again after the upgrade. For more information, see the section **Running Inventory Jobs** for steps to run the inventory on demand.

If the IP address of the new OpenManage Integration version 2.0 appliance has changed from that of the old appliance, the trap destination for the SNMP traps must be configured to point to the new appliance. For 12G servers, this will be fixed by running the Inventory on these hosts. For all 11G or lower generation hosts that were earlier complaint, this IP change will show up as non-complaint and will require configuring OMSA. For more information, see the section, **Running the Fix Non-Compliant vSphere hosts Wizard** to fix the host compliance in the this guide.

How to recover if I have unregistered the older plugin after the backup

If you have unregistered the plug-ins after taking backup of the database of the older version, perform the following steps before proceeding with the migration.

NOTE: Unregistering the plug-in has removed all the customizing that was done on the registered alarms by the plug-in. The following steps will not be able to restore the customizing, however, it will re-register the alarms in the default state.

1. Perform the steps 3-5 in the section **Migration Path to migrate from 1.6/1.7 to 2.0** in this chapter.
2. Register the plug-in to the same vCenters that you had registered earlier in the older plug-in.
3. Proceed with step 6 through step 9 in the section **Migration Path to migrate from 1.6/1.7 to 2.0** in this chapter to complete the migration. For more information, see the section **Migration Path to migrate from 1.6/1.7 to 2.0** in **OpenManage Integration Version 2.0 Quick Install Guide**.

8

About Logs

You can view user actions on the **Monitor** → **Log** tab of the OpenManage Integration for VMware vCenter.

You can sort the content on this page using the two drop-down lists. The first drop-down list lets you sort on file category, which includes:

- All Categories
- Info
- Warning
- Error
- Security

The second drop-down helps you sort on blocks of time, which include:

- Last Week
- Last Month
- Last Year
- Custom Range

  If you select custom range, you can pick the start and end date and click Apply.

You can also sort the datagrid columns in ascending or descending order by clicking the column header.

Use the Filter text box to search within your content.

At the bottom of the page grid, the following information is displayed:

Total items	Displays the total count of all log items.
Items per screen	Displays the number of log items on the displayed page. Use the drop-down box to set the number of items per page.
Page	Displays the page you are on. Type a page number in the text box or use the Previous and Next buttons to get you the page you want.
Previous or Next buttons	Buttons that guide you to the next or previous pages.
Export icon	Use this to export log content to a CSV file.

Viewing the Logs

1. In OpenManage Integration for VMware vCenter, click the **Monitor** tab.
2. On the Log tab, view the user actions logs for the OpenManage Integration for VMware vCenter. The Log page shows:

Category	Displays the category type.
Date and Time	Displays the date and time of the user action.
Description	Displays a description of the user action.

3. To sort the data in the grid, click a column header.
4. To sort using categories or time blocks use the drop-down lists above the grid.
5. To page between pages of log items, use the Previous and Next buttons.

Exporting Log Files

The OpenManage Integration for VMware vCenter uses a comma-separated values (CSV) file format for exporting information from data tables.

1. In OpenManage Integration for VMware vCenter, click the **Monitor** tab.
2. On the Log tab, view the user actions for the OpenManage Integration for VMware vCenter.
3. To export a CSV formatted log file, in the lower right-hand corner of the screen, click the **Export All** button.
4. In the **Select location for download** dialog box, browse to the location to save the log information.
5. In the File name text box, either accept the default name ExportList.csv or type your own file name.
6. Click **Save**.

9

Settings

The Settings tab is used to do the following:

- Editing the OMSA Link
- Viewing Warranty Expiration Notification Settings
- Configuring Warranty Expiration Notification
- Setting Up The Firmware Update Repository
- Viewing the Alarm and Event Settings
- Configuring and Managing Events and Alarms
- Viewing the Data Retrieval Schedules for Inventory and Warranty

Editing the OMSA Link

This procedure assumes that you have already installed an OMSA Web Server and that you have previously configured this link using the Configuration Wizard. See the *Dell OpenManage Server Administrator Installation Guide* for the version of OMSA in use and for instructions on how to install and configure the Web Server.

If you have not provided a link while running the Configuration Wizard, you can edit this link in OpenManage Integration for VMware vCenter **Manage** → **Settings** tab.

NOTE: OMSA is only required on Dell PowerEdge 11th generation servers or earlier.

1. In the OpenManage Integration for VMware vCenter, on the **Manage** → **Settings** tab, under vCenter Settings and to the right side of the OMSA Web Server URL, click **Edit**.
2. In the OMSA Web Server URL dialog box, type the **URL**.
   You must include the full URL including the HTTPS.
3. Select **Apply these settings to all vCenters** check box to apply the OMSA URL to all vCenters. If you do not select this check box, the OMSA URL is applied only to only one vCenter.
4. Verify that the link works by navigating to the host Summary tab for this host. Verify that the OMSA Console link is live within the Dell Host Information.

Understanding Using OMSA with 11th Generation Servers

On servers earlier than Dell PowerEdge 12th generation servers, you must install OMSA to work with the Dell OpenManage Integration for VMware vCenter. You can install OMSA automatically on Dell PowerEdge 11th generation hosts during deployment, or if you want to install it manually, you may still do so.

To configure OMSA on Dell PowerEdge 11th generation hosts, choose from the following:

- Deploying the OMSA Agent onto an ESXi System
- Deploying the OMSA Agent onto an ESX System
- Setting up an OMSA Trap Destination

- Editing the OMSA Link

Deploying The OMSA Agent Onto An ESXi System

Install the OMSA VIB on an ESXi system to gather inventory and alert information from the systems.

NOTE: Dell OpenManage agents are required on Dell hosts earlier than version 12G. You can install OMSA using the Dell Management Plug-in or manually to hosts prior to installing the Dell Management Plug-in. Details on manually installing the agents are at **http://support.dell.com/support/edocs/software/eslvmwre/sysman/sysman.htm** Open the guide for the appropriate version of ESX/ESXi software, and look for the "*Installing the Dell OpenManage Server Administrator*" chapter.

1. If not already installed, install the vSphere command line tool (vSphere CLI) from **http://www.vmware.com**.
2. Enter the following command:

   ```
   Vihostupdate.pl -server <IP Address of ESXi host> -i -b OM-SrvAdmin-Dell-Web-6.3.0-2075.VIB-ESX41i_A00.8.zip
   ```

   NOTE: It can take a few minutes for OMSA to install. This command requires a reboot of the host after it completes.

Deploying the OMSA Agent onto an ESX System

Install the OMSA tar.gz on an ESX system to gather inventory and alert information from the systems.

NOTE: Dell OpenManage agents are required on Dell hosts earlier than version 12G. You can install OMSA using the Dell Management Plug-in or manually to hosts prior to installing the Dell Management Plug-in. Details on manually installing the agents are at **http://support.dell.com/support/edocs/software/eslvmwre/sysman/sysman.htm** Open the guide for the appropriate version of ESX/ESXi software, and look for the "*Installing the Dell OpenManage Server Administrator*" chapter.

To deploy the OMSA agent tar.gz on an ESX system with the required remote enablement setting (-c) option:

1. Run the OMSA agent installation script:

   ```
   srvadmin-install.sh -x -c
   ```

2. Start OMSA services:

   ```
   srvadmin-services.sh start
   ```

3. If the OMSA agent is already installed, make sure that it has remote enablement configuration (-c) option or theOpenManage Integration for VMware vCenter installation will not complete successfully. Reinstall it with the -c option and restart the service:

   ```
   srvadmin-install.sh -c
   srvadmin-services.sh restart
   ```

Setting Up An OMSA Trap Destination

This task is only for host systems using OMSA for event generation instead of iDRAC6. There is no additional configuration required for iDRAC6.

NOTE: OMSA is only required on Dell servers earlier than version Dell PowerEdge 12th generation servers.

1. Either use the link to the OMSA user interface found in the OpenManage Integration for VMware vCenter **Manage** → **Settings** tab, or navigate to the OMSA agent from a Web browser (**https://<HostIP>:1311/**).
2. Log in to the interface, and select the **Alert Management** tab.

3. Select **Alert Actions** and make sure that any events to be monitored have the **Broadcast Message** option set, so that the events are sent out.
4. At the top of the tab, select the **Platform Events** option.
5. Click the grey **Configure Destinations** button, and click the **Destination** link.
6. Select the **Enable Destination** check box.
7. Enter the OpenManage Integration for VMware vCenter appliance IP address in the **Destination IP Address** field.
8. Click **Apply Changes**.
9. Repeat step 1 to step 8 to configure additional events.

10

Viewing Warranty Expiration Notification Settings

1. In the OpenManage Integration for VMware vCenter, on the **Manage** → **Settings** tab, under Appliance Settings, click **Warranty Expiration Notification**.
2. Under Warranty Expiration Notification you can view the following:
   - Whether the setting is enabled or disabled
   - The number of days for the first Warning setting.
   - The number of days for the Critical warning setting.
3. To configure Warranty Expiration Notification, see Configuring Warranty Expiration Notifications.

Configuring Warranty Expiration Notification

You can configure warranty expiration thresholds to warn about warranty expiration.

1. In the OpenManage Integration for VMware vCenter, on the **Manage** → **Settings** tab, under Appliance Settings, to the right side of **Warranty Expiration Notification**, click the **Edit** icon.
2. In the Warranty Expiration Notification dialog box, do the following:
   a) If you want to enable this setting, select the **Enable warranty expiration notification for hosts** check box.
   Selecting the check box enables warranty expiration notification.
   b) Under Minimum Days Threshold Alert, do the following:
      1. In the Warning drop-down list, select the number of days before you want to be warned of the warranty expiration.
      2. In the Critical drop-down list, select the number of days before you want to be warned of the warranty expiration.
3. Click **Apply**.

11

About Firmware Updates

The location where servers receive firmware updates is a global setting that is available in the OpenManage Integration for VMware vCenter on the Settings tab.

Firmware repository settings contain the firmware catalog location used to update deployed servers. There are two location types:

Dell (ftp.dell.com)	Uses the firmware update repository of Dell (**ftp.dell.com**). The OpenManage Integration for VMware vCenter downloads selected firmware updates from Dell.
Shared Network Folder	Created with Dell Repository Manager™. These local repositories are located on CIFS or NFS file share.

NOTE: Once the repository is created, save it to a location that the registered hosts can access. Repository passwords cannot exceed 31 characters. Do not use any of the following characters in a password: @, &, %, ', ", , (comma), < >

The Firmware Update Wizard always checks for the minimum firmware levels for iDRAC, BIOS, and Lifecycle Controller, and attempts to update them to required minimum versions. Once iDRAC, Lifecycle Controller, and BIOS firmware versions meet minimum requirements, the Firmware Update wizard allows updates for all firmware including: iDRAC, Lifecycle Controller, RAID, NIC/LOM, Power Supply, BIOS, and so on.

NOTE: For 9th and 10th generation servers, BIOS/BMC/DRAC firmware versions are viewable only at the Cluster View level in vCenter or on the Overview page of the individual host view. Firmware version information is not active in the individual host view under Firmware, and that page appears grayed out, and remote firmware updates are not available.

Firmware Versions After October 14, 2010

For Firmware updated on or after October 14th, 2010, the Firmware Update Wizard runs.

Firmware Versions Newer Than July 29, 2009 and Prior to October 14th

If your firmware was updated on or after July 29, 2009 and prior to October 14, 2010, you still will not see the Firmware Update Wizard, but you are delivered an ISO bundle to update your firmware. After this update, you may not have the latest firmware. After you run the bundle, it is recommended that you run the update again.

Firmware Versions Older than July 29, 2009

If your firmware is older than July 29, 2009, you may have to download and run the ISO file to update your machines. After you run the ISO, it is recommended that you run the Firmware Update Wizard again.

Related Information:

- Setting Up The Firmware Repository

Setting Up the Firmware Update Repository

You can set up the firmware update repository on the OpenManage Integration for VMware vCenter Settings tab.

1. In OpenManage Integration for VMware vCenter, on the **Manage** → **Settings** tab, under Appliance Settings and to the right side of Firmware Update Repository, click the **Edit** icon.
2. In the Firmware Update Repository dialog box, select one of the following:

– Dell Online

  Default firmware repository (ftp.dell.com) with a staging folder. The OpenManage Integration for VMware vCenter downloads selected firmware updates and stores them in the staging folder, and then you need to run the firmware wizard to update the firmware.

– Shared Network Folder

  These are created with the Dell Repository Manager application. Locate these local repositories on Windows-based file shares. Use the live link to go to Dell Repository Manager.

3. If you selected **Shared Network Folder** , do the following:
   a) Enter the **Catalog File Location** using the following format:
      * NFS share for xml file: host:/share/filename.xml
      * NFS share for gz file: host:/share/filename.gz
      * CIFS share for xml file: \\host\share\filename.xml
      * CIFS share for gz file: \\host\share\filename.gz
   b) If the downloading of the files are in progress in the selected repository path which is displayed in the **Select Update Source** screen, an error message is displayed notifying that the download is in progress.
4. When the test is complete, click **Apply**.

Running The Firmware Update Wizard for a Single Host

This functionality is only available for 11th and 12th generation Dell servers that have either an iDRAC Express or Enterprise card. When your firmware was installed on or after October 14th, 2010, you can automatically update your firmware versions using the Firmware Update Wizard.

NOTE: To safeguard against browser timeout issues, change the default timeout to 30 seconds. For information on changing the default timeout setting, see How Come I see an Error Message Displayed After Clicking the Firmware Update Link in the Troubleshooting section of the *User's Guide*.

NOTE: Right click on **Host** > **All OpenManage Integration Actions** > **Firmware Update** to access the firmware wizard. Or, Click on **Host** > **Actions** > **All OpenManage Integration Actions** > **Firmware Update** to access the firmware wizard. Or, Click on **Host** > **Summary** > **Dell Host Information** > **Firmware Update** to access the firmware wizard.

NOTE:

To run the Firmware Update Wizard:

1. In the **vSphere Web Client** click on **Hosts**. The list of available hosts are displayed.
2. Select a host from the displayed list. If there is only one host then only one host is displayed.
3. In the main menu, click on **Monitor** and then select the **Dell Host Information** tab. The inventory information of the Dell Hosts are displayed.
4. Click on **Firmware**, the available firmwares with the details are displayed.
5. Click on **Run Firmware Wizard**. The **Firmware Update** screen is displayed.
6. Click **Next**, the **Select Update Source** screen is displayed with the firmware update bundle for the given host is displayed.
   a) In the screen, select the firmware update bundle from the **Select an Update Bundle** drop-down list.
7. Click **Next**. The **Select Components** screen is displayed which lists the firmware details for the components.
8. Select the desired firmware updates and click **Next**. Components that are either a downgrade or currently scheduled for update are not selectable. If you select the **Allow Firmware downgrade** check box, select the options that are listed as Downgrade. Selecting this option is only recommended to advanced users who understand the implications of downgrading firmware.

9. Click **Next.** The **Schedule Firmware Update** screen is displayed.
   - Enter the job name in the **Firmware Update Job Name** field and description in the **Firmware Update Description** field. This field entry is optional.
   - Select **Update Now** will start the firmware update job immediately.
   - **Schedule Update** button , select this radio button to run the firmware update job later and click on **Next**. You can schedule the firmware update job after 30 minutes from the current time.
   - In the Calendar box, select the month and day.
   - In the Time text box, type the time in HH:MM, and then click Next. The time is the local time zone where your client is physically located. Invalid time values result in a blocked update.
   - **Apply updates on next reboot.**

     To avoid a service interruption, it is recommended that the host enters maintenance mode before the reboot.
   - **Apply updates and force reboot without entering maintenance mode.**

     -The update is applied, and a reboot occurs even if the host is not in maintenance mode. This method is not recommended.
10. Click **Next**. The **Summary** page is displayed that provides details about all components after firmware update.
11. Click **Finish**.
12. To verify that the update was successful, in **Monitor** tab, select **Job Queue** → **Firmware Updates**, and review the **OpenManage Integration Overview** page to see the new versions.

Running the Update Firmware Wizard for a Cluster

This functionality is only available for 11th and 12th generation Dell servers that have either an iDRAC Express or Enterprise card. If your firmware was installed on or after October 14th, 2010, you can automatically update your firmware versions using the Firmware Update Wizard. This wizard only updates hosts that are part of a connection profile and compliant in terms of firmware, CSIOR status, hypervisor, and OMSA status (11th generation servers only). Select a cluster that is listed in the Clusters view and use the Firmware Update Wizard. It typically takes from 30 to 60 minutes to update firmware components for each cluster. Enable DRS on a cluster so that virtual machines can be migrated when a host enters/exits maintenance mode during the firmware update process. You can only schedule or run one firmware update task at a time.

If you want to export from the wizard, use the Export to CSV button. Search is available for locating a specific cluster, datacenter, host, or any topic item from the datagrid except for Date Applied.

NOTE: Always update firmware together as part of the repository bundle: BIOS, iDRAC, and Lifecycle Controller.

NOTE: For information on changing the default timeout setting, see the Troubleshooting section of the *User's Guide*.

You can view the status and manage Firmware update jobs from the Job Queue page. See, Viewing Firmware Details for Datacenters and Clusters.

1. Click on **OpenManage Integration** icon, click on **Clusters** hat is displayed in the left pane. The list of clusters are displayed.
2. Click on a cluster from the displayed list. The main menu is displayed with different options.
3. Click on **Monitor** -->**Dell Cluster Information** -->**Firmware**. The **Run Firmware Wizard** screen is displayed.
4. Click on **Run Firmware Wizard** link. The **Welcome** Page is dislayed.
5. Click **Next**. The **Select Update Source** screen is displayed where you can select the bundles. The Repository location is also displayed.
6. Select host from the displayed list in the **Select Bundles** area. You should select at least one bundle for firmware update. Each host has a drop-down list next to the host name from which you can select the required bundle.

7. Click **Next**. The **Select Components** screen is displayed. This screen displays the details of components such as model name, host name, service tag, component and so on for the selected host.
8. Select at least one component from the list, and click **Next** to proceed. You can filter the content of the component data grid using the **Filter** field or, drag and drop columns within the component data grid. If you select the **Allow Firmware downgrade** check box, the existing firmware version will roll back to the previous available version.
9. Click **Next**, the **Schedule Firmware Update** screen is displayed.
   a) Enter the firmware update job name in the **Firmware Update Job Name** field. This value is mandatory.
   b) Enter the firmware update description in the **Firmware Update Description** field. This value is optional.
10. Select an option from the following.
    a) **Update Now**, select this radio button to run the firmware update job now and click on **Next**.
    b) **Schedule Update** button , select this radio button to run the firmware update job later and click on **Next**. You can schedule the firmware update job after 30 minutes from the current time.
    c) In the **Calendar** box, select the month and day.
    d) In the **Time** text box, type the time in HH:MM, and then click **Next**. The time is the local timezone where your client is physically located. Invalid time values result in a blocked update.
11. The **Summary** screen is displayed with all the firmware update details.
12. Click **Finish** and a message The **firmware update job has been created** for successful firmware update is displayed.

12

Understanding Events And Alarms

You can edit events and alarms from the OpenManage Integration for VMware vCenter within **Manage** → **Settings** tab. From here you can select the Event Posting Level, enable Alarms for Dell Hosts, or Restore Default Alarms. You can configure events and alarms for each vCenter or all at once for all registered vCenters.

NOTE: To receive Dell events, you must enable both alarms and events.

There are four event posting levels.

Table 2. Event Posting Level Descriptions

Event	Description
Do not post any Events	Do not have the OpenManage Integration for VMware vCenter forward any events or alerts into related vCenters.
Post all Events	Post all events, including informal events, that the OpenManage Integration for VMware vCenter receives from managed Dell hosts into related vCenters.
Post only Critical and Warning Events	Posts only events with either Critical or Warning criticality into related vCenters.
Post only Virtualization-Related Critical and Warning Events	Post Virtualization related events received from hosts into related vCenters. Virtualization related events are those that Dell has selected to be most critical to hosts running virtual machines.

When you configure your events and alarms, you can enable them. When enabled, critical hardware alarms can trigger the OpenManage Integration for VMware vCenter to put the host system into a maintenance mode, and in certain cases, migrate the virtual machines to another host system. The OpenManage Integration for VMware vCenter forwards events received from managed Dell hosts, and creates alarms for those events. Use these alarms to trigger actions from vCenter, like a reboot, maintenance mode, or migrate. For example, when a dual power supply fails and an alarm is created, the resulting action is to migrate the virtual machine on that machine to a new one.

A host enters or leaves maintenance mode only as when you request it. If the host is in a cluster when it enters maintenance mode, you are given the option to evacuate powered-off virtual machines. If this option is selected, each powered-off virtual machine is migrated to another host, unless there is no compatible host available for the virtual machine in the cluster. While in maintenance mode, the host does not allow deployment or *power-on* of a virtual machine. Virtual machines that are running on a host entering maintenance mode need to be either migrated to another host or shut down, either manually or automatically by VMware Distributed Resource Scheduling (DRS).

Any hosts outside of clusters, or in clusters without VMware Distributed Resource Scheduling (DRS) enabled, could see virtual machines being shut down due to a critical event. DRS continuously monitors usage across a resource pool and intelligently allocates available resources among virtual machines according to business needs. Use clusters with DRS configured in conjunction with Dell Alarms to make sure that virtual machines are automatically migrated on critical hardware events. Listed in the details of the on screen message are any clusters on this vCenter instance that may be impacted. Confirm that the clusters are impacted before enabling Events and Alarms.

If you ever need to restore the default alarm settings, you can do so with the Reset Default Alarm button. This button is a convenience to restore the default alarm configuration without uninstalling and reinstalling the product. If any Dell alarm configurations have been changed since install, those changes are reverted using this button.

NOTE: The OpenManage Integration for VMware vCenter pre-selects the virtualization-related events that are the essential to hosts successfully running virtual machines. Dell host alarms are disabled by default. If Dell alarms are enabled, the clusters should use the VMware Distributed Resource Scheduler to make sure that the virtual machines that send critical events are automatically migrated.

Configuring Events And Alarms

For detailed information about events and alarms see Understanding Alarms and Events. Configure events and alarms on the OpenManage Integration for VMware vCenter **Management** → **Settings** tab. Under vCenter Settings, expand the Events and Alarms heading to display the current vCenter Alarms for Dell Hosts (Enabled or Disabled), or for all and the Event Posting Level.

NOTE: On hosts prior to Dell PowerEdge 12th generation servers, this feature requires that the virtual appliance is configured as a trap destination in OMSA to display host events in vCenter. For more information on OMSA, see Setting Up An OMSA Trap Destination.

NOTE: To receive Dell events, you must enable both alarms and events.

1. In the OpenManage Integration for VMware vCenter **Manage** → **Settings** tab, next to vCenter Settings use the drop-down list to select the vCenter server or All vCenter Servers to included with this setting.

   If you selected All Registered Servers, the options may display blank. This lets you configure the settings for all the registered vCenters at once. If the vCenters had the same settings, they will appear.
2. To the right side of Events and Alarms, click the **Edit** icon.
3. To enable all hardware alarms and events, select the **Enable Alarms for all Dell Hosts** check box.

   NOTE: Dell hosts that have alarms enabled respond to critical events by entering maintenance mode and you can modify the alarm as needed.
4. To restore the default vCenter alarm settings for all managed Dell servers, click **Restore Default Alarms**.

   It may take up to a minute before the change takes effect.
5. Under **Event Posting Level**, select one of the following:

   - Do not post any events

     This options blocks hardware events.
   - Post All Events

     This option posts all hardware events.
   - Post only Critical and Warning Events

     This option posts only critical or warning level hardware events.
   - Post only Virtualization-Related Critical and Warning Events

     This option posts only virtualization-related critical and warning events. This is the default event posting level.
6. If you want to apply these settings to all vCenters, select the **Apply these settings to all vCenters** check box.

   NOTE: Selecting this option overrides the existing settings for all vCenters.

   This option is grayed out if you already selected All Registered vCenters from the drop-down list on the Setting page.
7. To save, click **Apply**.

Viewing Events

Configure events before you can view them in the Events tab, see Configuring Events and Alarms.

View the events for a host, cluster or datacenter on the Events tab.

1. In OpenManage Integration for VMware vCenter, in the Navigator, click **Hosts**, **Datacenter** or **Clusters**.
2. On the Objects tab, select the specific host, datacenter or cluster for which you want to view events.
3. On the Monitor tab, click **Events**.
4. To view more event details, select a specific event.

Viewing the Alarm and Event Settings

Once alarms and events are configured you can view if the vCenter alarms for hosts are enabled and which event posting level is selected on the Settings tab.

1. In the OpenManage Integration for VMware vCenter**Manage** → **Settings** tab, under vCenter Settings, expand Events and Alarms.
2. Under Events and Alarms you can view the following:
   - vCenter Alarms for Dell Hosts: Displays either Enabled or Disabled.
   - Event Posting Level

     To see the event posting levels that can display, see Understanding Alarms and Events.
3. To configure alarms and events, see Configuring Events and Alarms

Viewing the Data Retrieval Schedules for Inventory and Warranty

1. In the OpenManage Integration for VMware vCenter, on the **Manage** → **Settings** tab, under vCenter Settings, click **Data Retrieval Schedule**.

   Clicking Data Retrieval Schedule expands to expose the schedules for inventory and warranty.
2. For either Inventory or Warranty Retrieval, view the settings:
   - Shows whether the option is enabled or disabled
   - Displays the week days for which it is enabled.
   - Displays the time of day it is enabled.
3. If you click **Data Retrieval Schedule** again, it rolls up the information into a single line and displays whether the option is enabled or disabled.
4. If you want to edit the Data Retrieval Schedule, see Modifying Inventory Job Schedules or Modifying a Warranty Job Schedule.

13

Monitoring a Single Host

The OpenManage Integration for VMware vCenter lets you view detailed information for a single host. You can access hosts in VMware vCenter from the left side Navigator. This displays all hosts for all vendors. Click on a specific Dell host to find more detailed information. To quickly view a list of Dell Hosts, from withinOpenManage Integration for VMware vCenter, in the left Navigator, click Dell Hosts.

- Viewing Host Summary Details
- Viewing Hardware: FRU Details for a Single Host
- Viewing Hardware: Processor Details for a Single Host
- Viewing Hardware: Power Supply Details for a Single Host
- Viewing Hardware: Memory Details for a Single Host
- Viewing Hardware: NICs Details for a Single Host
- Viewing Hardware: PCI Slot Details for a Single Host
- Viewing Hardware: Remote Access Card Details for a Single Host
- Viewing Storage Details for a Single Host
  - Viewing Storage: Virtual Disk Details for a Single Host
  - Viewing Storage: Physical Disk Details for a Single Host
  - Viewing Storage: Controller Details for a Single Host
  - Viewing Storage: Enclosure Details for a Single Host
- Viewing Firmware Details for a Single Host
- Viewing Power Monitoring for a Single Host
- Viewing Warranty Status for a Single Host
- Quickly Viewing Only Dell Hosts

Viewing Host Summary Details

View the host summary details for an individual host on the Host Summary page. This page displays various portlets. Two apply to the OpenManage Integration for VMware vCenter specially and you can drag and drop the portlets to the position you want.

1. In the OpenManage Integration for VMware vCenter, in the Navigator, click **Hosts**.
2. In the Objects tab, select the specific host you want to review.
3. Click the **Summary** tab.
4. View the host summary details:

Summary Information — At the top of this page, in the upper left corner is a summary list of information for this host.

Alerting system — If there are alerts for the OpenManage Integration for VMware vCenter, they display in a yellow box below the status area and above the portlets.

Notification area — Dell products integrate information in this right side-panel area. You can find information about:

- Recent Tasks
- Work In Progress
- Alarms

  Dell alarm information displays in this notification area portlet.

5. Scroll down to view the Dell Server Management portlet.

Service Tag — The Service Tag for your Dell PowerEdge server. Use this number when you call for support.

Model Name — Displays the .servers model name.

Fault Resilient Memory — This is a BIOS attribute and is enabled in the BIOS during initial setup of the sever and displays the memory operational mode of the server. You need to restart your system when you change memory operational mode value. This is applicable for R620, R720, T620, M620 servers with ESXi 5.5 or later version. The four different values are:

- Enabled and Protected: This value indicates that the system is supported and operating system version is ESXi 5.5 or later and the memory operational mode in BIOS is set to FRM.
- Enabled and Not Protected: This value indicates that it supports the system with operating system version lesser than ESXi 5.5.
- Disabled: This value indicates that it supports valid systems with any operating system version and here memory operational mode in BIOS is not set to FRM.
- Blank: If memory operational mode in BIOS is not supported the FRM attribute is not displayed.

Identification

- Host name

  The name of your Dell host.
- Power State

  Displays if your power is ON or OFF.
- iDRAC IP

  Displays the iDRAC IP address.
- Management IP

  Displays the management IP address.
- Connection Profile

  Displays the connection profile name for this host.
- Model

  Displays the Dell server model.
- Service Tag

  Displays the Service Tag for the server.
- Asset Tag

Displays the asset tag.

- Warranty Days Left
  Displays the days left for the warranty.
- Last Inventory Scan
  Displays the date and time of the last inventory scan.

Hypervisor & Firmware

- Hypervisor
  Displays the Hypervisor version.
- BIOS Version
  Displays the BIOS version.
- Remote Access Card Version
  Displays the remote access card version.

Management Consoles — The management consoles are used to launch external system management consoles, such as:

- Remote Access Console (iDRAC)
  Launches the Integrated Dell Remote Access Controller (iDRAC) web user interface.
  To configure the OMSA link, see Editing the OMSA Link.
  Launches the OpenManage Server Administrator (OMSA) user interface if it has been configured.

Host Actions — Blink Indicator Light lets you set up your physical server to blink at various time intervals.

6. View the Dell Host Health portlet:

Dell Host Health — Component health is a graphical representation of the status of all major host server components: main system chassis, power supply, temperature, fans, voltage, processors, batteries, intrusion, hardware log, power management, and memory. Options include:

- Healthy (green check mark) - component operating normally
- Warning (yellow triangle with exclamation point) - component has a non-critical error
- Critical (red X) - component has a critical failure
- Unknown (question mark) - status is unknown for the component

Launching Management Consoles

There are two management consoles you can launch from the Dell Server Management Portlet. These include:

- Remote Access Console (iDRAC Console)
  Launch the Remote Access Console to access the iDRAC user interface.
- OMSA Console.
  Launch the OMSA Console to launch the OpenManage Server Administrator user interface URL that was entered into the Configuration Wizard. You must install the URL for the server administrator Web server on a Windows-based management station.

Launching the Remote Access Console (iDRAC)

You can launch the iDRAC user interface from the Dell Server Management Portlet.

1. In the OpenManage Integration for VMware vCenter, in the Navigator area, under Inventory Lists, click **Hosts**.
2. On the Object tab, double-click the host you want.
3. On the Summary tab, scroll down to the Dell Server Management portlet.
4. Click **Management Consoles → Remote Access Console (iDRAC)**.

Setting Up Physical Server Blink Indicator Light

To assist in locating a physical server in a large datacenter environment, you can set the front indicator light to blink for a set time period.

1. In the OpenManage Integration for VMware vCenter, in the Navigator area, under Inventory Lists, click **Hosts**.
2. On the Object tab, double-click the host you want.
3. On the Summary tab, scroll down to the Dell Server Management portlet.
4. Under **Host Actions**, select **Blink Indicator Light**.
5. Choose one of the following:
   - To turn the blink on and set the time period, in the **Indicator Light** dialog box, click **Blink On**, and use the Timeout drop-down list to select the timeout increment, and then click **OK**.
   - To turn the blink off, in the **Indicator Light** dialog box, click **Blink Off**, and then click **OK**.

14

Buying and Uploading a Software License

You are running a trial license until you upgrade to a full product version. Use a *Buy License* link from the product to navigate to the Dell website and buy a license. Once you buy it, upload it using the Administration Console. This option only appears if you are using a trial license.

1. In the OpenManage Integration for VMware vCenter. Do one of the following:
   - On the **Licensing** tab, next to Software License, click **Buy License**.
   - On the Getting Started tab, under Basic Tasks, click **Buy License**.

     NOTE: The license will be sent by e-mail as an XML file. For licensing quires send an e-mail with original order number to **download_software@dell.com**.
2. In the Dell web page, purchase your license and save the file to a known location.
3. In a web browser, type the Administration Console URL.
   Use the format: https://<ApplianceIPAddress>
4. In the Administration Console login window, type the password and click **Login**.
5. Click **Upload** license.
6. In the Upload License window, to navigate to the license file, click **Browse**.
7. Select the license file and then click **Upload**.

About OpenManage Integration for VMware vCenter Licensing

The OpenManage Integration for VMware vCenterhas two types of licenses:

Evaluation license	The trial version contains a evaluation license for five hosts (servers) that are managed by the OpenManage Integration for VMware vCenter.This is applicable only for 11G and later generations. This is a default license and is for a 90 days trial period only.
Standard license	The full product version contains a standard license for up to ten vCenters and you can purchase any number of host connections that are managed by the OpenManage Integration for VMware vCenter.

When you upgrade from a evaluation license to a full standard license, a new license XML file is sent to you by e-mail. Save the file to your local system and upload the new license file using the Administration Console. Licensing presents the following information:

- Maximum vCenter Connection Licenses - up to ten registered and in use vCenter connections are allowed.
- Maximum Host Connection Licenses - the number of host connections that were purchased.
- In Use - the number of vCenter connection or host connection licenses in use. For host connection, this number represents the number of hosts (or servers) that have been discovered and inventoried.
- Available - the number of vCenter connection or host connection licenses available for future use.
- Unlicensed Hosts - The number of host connections that exceeded the licensed amount. The OpenManage Integration for VMware vCenter continues to function normally, but a new license must be purchased and installed to resolve this warning

NOTE: The standard license period is for 3 years only and the additional licenses will be appended to the existing license and not over written. You cannot add 9g\10g to a new or existing connection profile if total number of 11g \12g hosts for which inventory ran successfully has reached the blocking number.

15
Viewing Hardware: FRU Details for a Single Host

View the Field Replaceable Unit (FRU) details for a single host on the Dell Host Information tab. For information to appear on this page, you must run an inventory job. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

1. In OpenManage Integration for VMware vCenter, in the Navigator, click **Hosts**.
2. On the Host tab, select the specific host for which you want to view Hardware: FRU details.
3. On the Monitor tab, select the **Dell Host Information** tab, and on the Hardware: FRU sub-tab, view the following:

Part Name	Displays the FRU part name.
Part Number	Displays the FRU part number.
Manufacturer	Displays the manufacturer's name.
Serial Number	Displays the Manufacturer's serial number.
Manufacture Date	Displays the manufacture date.

16

Viewing Hardware: Processor Details for a Single Host

View the processor details for a single host on the Dell Host Information tab. For information to appear on this page, you must run an inventory job. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

1. In OpenManage Integration for VMware vCenter, in the Navigator, click **Hosts**.
2. On the Object tab, select the specific host for which you want to view processor details.
3. On the Monitor tab, select the **Dell Host Information** tab, and on the Hardware: Processor sub-tab, view the following:

Socket	Displays the slot number.
Speed	Displays the current speed.
Brand	Displays the processor brand.
Version	Displays the processor version.
Cores	Displays the number of cores in this processor.

17

Viewing Hardware: Power Supply Details for a Single Host

View the virtual power supply details for a single host on the Dell Host Information tab. For information to appear on this page, you must run an inventory job. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

1. In OpenManage Integration for VMware vCenter, in the Navigator, click **Hosts**.
2. On the Objects tab, select the specific host for which you want to view Hardware: Power Supply details.
3. On the Monitor tab, select the **Dell Host Information** tab, and on the **Hardware: Power Supply** sub-tab, view the following:

Type	Displays the type of power supply. Power supply types include: – UNKNOWN – LINEAR – SWITCHING – BATTERY – UPS – CONVERTER – REGULATOR – AC – DC – VRM
Location	Displays the location of the power supply, such as Slot 1.
Output (Watts)	Displays the power in Watts.

18

Viewing Hardware: Memory Details for a Single Host

View the memory details for a single host on the Dell Host Information tab. For information to appear on this page, you must run an inventory job. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

1. In OpenManage Integration for VMware vCenter, in the Navigator, click **Hosts**.
2. On the Objects tab, select the specific host for which you want to view Hardware: Memory details.
3. On the Monitor tab, select the **Dell Host Information** tab, and on the **Hardware: Memory** sub-tab, view the following:

Memory Slots	Displays the Used, Total, and Available memory count.
Memory Capacity	Displays the Installed Memory, Total Memory Capacity, and Available Memory.
Slot	Displays the DIMM slot.
Size	Displays the memory size.
Type	Displays the memory type.

19

View Hardware: NICs Details for a Single Host

View the Network Interface Card (NIC) details for a single host on the Dell Host Information tab. For information to appear on this page, you must run an inventory job. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

1. In OpenManage Integration for VMware vCenter, in the Navigator, click **Hosts**.
2. On the Objects tab, select the specific host for which you want to view Hardware: NICs details.
3. On the Monitor tab, select the **Dell Host Information** tab, and on the **Hardware: NICs** sub-tab, view the following:

Total	Displays the total count of available network interface cards.
Name	Displays the NIC name.
Manufacturer	Displays only the manufacturer name.
MAC Address	Displays the NIC MAC address.

20

Viewing Hardware: PCI Slots for a Single Host

View the PCI slot details for a single host on the Dell Host Information tab. For information to appear on this page, you must run an inventory job. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

1. In OpenManage Integration for VMware vCenter, in the Navigator, click **Hosts**.
2. On the Objects tab, select the specific host for which you want to view Hardware: PCI Slot details.
3. On the Monitor tab, select the **Dell Host Information** tab, and on the **Hardware: PCI Slots** sub-tab, view the following:

PCI Slots	Displays the Used, Total, and Available PCI slots.
Slot	Displays the slot.
Manufacturer	Displays the manufacturer name of the PCI slot.
Description	Displays the description of the PCI device.
Type	Displays the PCI slot type.
Width	Displays the data bus width, if available.

21

Viewing Hardware: Remote Access Card Details for a Single Host

View the Remote Access Card details for a single host on the Dell Host nformation tab. For information to appear on this page, you must run an inventory job. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

1. In OpenManage Integration for VMware vCenter, in the Navigator, click **Hosts**.
2. On the Objects tab, select the specific host for which you want to view Hardware: Remote Access Card details.
3. On the Monitor tab, select the **Dell Host Information** tab, and on the **Hardware: Remote Access Card** sub-tab, view the following:

IP Address	Display the IP address for the remote access card.
MAC Address	Displays the MAC address for the remote access card.
RAC Type	Displays the type of the remote access card.
URL	Displays the live URL for the iDRAC associated with this host.

22

Viewing Storage Details for a Single Host

View the storage details for a single host on the Dell Host Information tab. For information to appear on this page, run an inventory job. See Running an Inventory Job Now. This page displays different options depending on what is selected from the View drop-down list. If you select Physical Disks, another drop-down list appears. This new drop-down list called Filter lets you filter your physical disk options.

NOTE: Hardware views are directly reporting the data from OMSA and iDRAC.

1. In OpenManage Integration for VMware vCenter, in the Navigator, click **Hosts**.
2. On the Objects tab, select the specific Host for which you want to view Storage: Physical Disk details.
3. On the Monitor tab, select the **Dell Host Information** tab, and on the **Storage** sub-tab, view the following:

Storage	Displays the counts of Virtual Disks, Controllers, Enclosures, and associated Physical Disks with its Global Hot Spare and Dedicated Hot Spare counts. When you selected from the View drop-down list, the option is highlighted here.
View	Displays the page options you want to view for this host: – Virtual Disks – Physical Disks – Controllers – Enclosures

Viewing Storage: Virtual Disk Details for a Single Host

The storage options on the Host Storage page depend on what you select from the View drop-down list.

If you selected Virtual Disks from the View drop-down list, view these options:

Name	Displays the name of the virtual disk.
Device FQDD	Displays the FQDD.
Physical Disk	Displays on which physical disk the virtual disk is located.
Capacity	Displays the capacity of the virtual disk.
Layout	Displays the layout type of the virtual storage. This means the type of RAID that was configured for this virtual disk.
Media Type	Displays either SSD or HDD.
Controller ID	Displays the controller ID.
Device ID	Displays the device ID.
Stripe Size	The stripe size refers to the amount of space that each stripe consumes on a single disk.

Bus Protocol This displays the technology that the physical disks included in the virtual disk are using. Possible values are:

- SCSI
- SAS
- SATA

Default Read Policy The default read policy supported by the controller. Options include:

- Read-Ahead
- No-Read-Ahead
- Adaptive Read-Ahead
- Read Cache Enabled
- Read Cache Disabled

Default Write Policy The default write policy supported by the controller. Options include:

- Write-Back
- Force Write Back
- Write Back Enabled
- Write-Through
- Write Cache Enabled Protected
- Write Cache Disabled

Cache Policy Displays if cache policy is enabled.

Viewing Storage: Physical Disk Details for a Single Host

The storage options on the Host Storage page depend on what you select from the View drop-down list. When you select this option the Filter drop-down list displays. You can filter your physical disks on the following options:

- All Physical Disks
- Global Hot Spares
- Dedicated Hot Spares
- The last option displays custom named virtual disks.

If you selected Physical Disks from the View drop-down list, view these options:

Name Displays the name of the physical disk.

Device FQDD Displays the device FQDD.

Capacity Displays the physical disk capacity.

Disk Status Displays physical disk status. Options include:

- ONLINE
- READY
- DEGRADED
- FAILED
- OFFLINE

- REBUILDING
- INCOMPATIBLE
- REMOVED
- CLEARED
- SMART ALERT DETECTED
- UNKNOWN
- FOREIGN
- UNSUPPORTED

Configured Displays whether the disk is configured.

Hot Spare Type Shows the hot spare type. Options include:

- No
  No means there is no hot spare.
- Global
  A global hot spare is an unused backup disk that is part of the disk group.
- Dedicated
  A dedicated hot spare is an unused backup disk that is assigned to a single virtual disk. When a physical disk in the virtual disk fails, the hot spare is activated to replace the failed physical disk without interrupting the system or requiring your intervention.

Virtual Disk Displays the name of the virtual disk.

Bus Protocol Displays the bus protocol.

Controller ID Displays the controller ID.

Connector ID Displays the connector ID.

Enclosure ID Displays the enclosure ID.

Device ID Displays the device ID.

Model Displays the model number of the physical storage disk.

Part Number Displays the storage part number.

Serial Number Displays the storage serial number.

Vendor Displays the storage vendor name.

Viewing Storage: Controller Details for a Single Host

The storage options on the Host Storage page depend on what you selected from the View drop-down list.

If you selected Controllers from the View drop-down list, view these options:

Controller ID Displays the controller ID.

Name Displays the name of the controller.

Device FQDD Displays the FQDD of the device.

Firmware Version	Displays the firmware version.
Minimum Required Firmware	Displays the minimum required firmware.
Driver Version	Displays the driver version.
Patrol Read State	Displays the Patrol Read State.
Cache Size	Displays the cache size.

Viewing Storage: Enclosure Details for a Single Host

The storage options on the Host Storage page depend on what you selected from the View drop-down list.

If you selected Enclosures from the View drop-down list, view these options:

Controller ID	Displays the controller ID.
Connector ID	Displays the connector ID.
Enclosure ID	Displays the enclosure ID.
Name	Displays the name of the enclosure.
Device FQDD	Displays the device FQDD.
Service Tag	Displays the Service Tag.

23

Viewing Firmware Details for a Single Host

View the firmware details for a single host on the Dell Host Information tab. For information to appear on this page, run an inventory job. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now. This host page lets you use the search filter and export a CSV file of firmware information.

1. In OpenManage Integration for VMware vCenter, in the Navigator, click **Hosts**.
2. On the Objects tab, select the specific host for which you want to view firmware details.
3. On the Monitor tab, select the **Dell Host Information** tab, and on the Firmware sub-tab, view the following:

Name	Displays the name of all the firmware on this host.
Type	Displays the type of firmware.
Version	Displays the version of all the firmware on this host.
Installation Date	Displays the installation date.

24

Viewing Power Monitoring for a Single Host

View the power monitoring details for a single host on the Dell Host Information tab. For information to appear on this page, run an inventory job. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

NOTE: Host time, as used here, means the local time where the host is located.

1. In OpenManage Integration for VMware vCenter, in the Navigator, click **Hosts**.
2. On the Objects tab, select the specific Host for which you want to view power monitoring details.
3. On the Monitor tab, select the **Dell Host Information Host** tab, and on the Power Monitoring sub-tab, view the following:

General Information	Displays the Power Budget and Current Profile name.
Threshold	Displays the Warning and Failure thresholds in Watts.
Reserve Power Capacity	Displays the Instant and Peak reserve power capacity in Watts.
	Energy Statistics
Type:	Displays the energy statistics type.
Measurement Start Time (Host Time)	Displays the date and time when the host began to consume power.
Measurement Finish Time (Host Time)	Displays the date and time when the host stopped to consume power.
Reading	This instantaneous value is the average value of readings over a one-minute time period.
Type:	Displays the energy statistics type.
Measurement Start Time (Host Time)	Displays the date and time when the host peak power began.
Peak Time (Host Time)	Displays the date and time of the host peak amps.
Peak Reading	The System Peak Power statistic is the peak power consumed by the system (in Watts).

25

Viewing Warranty Status for a Single Host

You must have run a warranty job to view a warranty status. See Running a Warranty Job Now.

View the warranty status details for a single host on the Dell Host Information tab. The Warranty Status page lets you monitor the warranty expiration date. Warranty settings control when server warranty information is retrieved from Dell online by enabling or disabling the warranty schedule and then setting the Minimum Days Threshold alert. See Warranty History.

1. In OpenManage Integration for VMware vCenter, in the Navigator, click or **Hosts**.
2. On the Objects tab, select the specific host for which you want to view warranty summary details.
3. On the Monitor tab, select the **Dell Host Information** tab, and on Warranty Summary sub-tab, view the following:

Renew Warranty button	Use this button to renew your warranty. See, Renewing Host Warranty
Provider	Displays the name of the provider for the warranty.
Description	Displays a description.
Status	Displays the warranty status of the host. Status options include: – Active The host is under warranty, and has not exceeded any threshold. – Warning The host is Active, but exceeded the warning threshold. – Critical Same as warning, but for a critical threshold. – Expired The warranty has expired for this host. – Unknown OpenManage Integration for VMware vCenter cannot get warranty status because the warranty job has not run, an error has occurred getting the data, or the system does not have a warranty.
Start Date	Displays the start date of the warranty.
End Date	Displays the end date of the warranty.
Days Left	Displays the days left on the warranty.
Last Updated	The last time the warranty was updated.

Renewing Host Warranty

Renew Host Warranty from the Host Warranty Details page.

1. In OpenManage Integration for VMware vCenter, in the Navigator, click **Hosts**.
2. On the Objects tab, select the specific host for which you want to renew host warranty.
3. On the Monitor tab, select the **Dell Host Information** tab, and on Warranty sub-tab, click **Renew Warranty**. This takes you to a web page where you can renew your warranty.

26

Quickly Viewing Only Dell Hosts

When you want to quickly view only Dell hosts, you can do this from within OpenManage Integration for VMware vCenter, and in the Navigator you can select Dell Hosts.

1. In VMware vCenter home page, click the OpenManage Integration icon.
2. In the Navigator, under OpenManage Integration for VMware vCenter, click Dell Hosts.
3. On the Dell Host tab, view the following information:

Host Name	Displays a link using the IP address for each Dell host. Click a specific host link to view the Dell host information.
vCenter	Displays the vCenter IP address for this Dell host.
Cluster	If this Dell host is in a cluster, the cluster name displays here.
Connection Profile	Displays the name of the connection profile.

27

Monitoring Hosts on Clusters and Datacenters

The OpenManage Integration for VMware vCenter lets you view detailed information for all hosts included in a datacenter or cluster. These pages let you sort data by clicking the data grid row header. Datacenter and cluster pages let you export information to a CSV file and offers filter/search functionality on the data grid. Details include:

- Viewing Host Overview Details
- Viewing Hardware: FRUs
- Viewing Hardware: Processor Details
- Viewing Hardware: Power Supply Details
- Viewing Hardware: Memory Details
- Viewing Hardware: NICs
- Viewing Hardware: PCI Slot Details
- Viewing Hardware: Remote Access Card Details
- Viewing Storage: Physical Disk Details
- Viewing Storage: Virtual Disk Details
- Viewing Firmware Details
- Viewing Power Monitoring
- Viewing Warranty Summary Details

28

Viewing Overview Details for Datacenters and Clusters

View the host details for datacenters or clusters on the Dell Datacenter/Cluster Information tab. For information to appear on this page, run an inventory job. The data you view may vary depending on which view you are accessing the data. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

NOTE: Datacenter and cluster pages let you export information to a CSV file and offers filter/search functionality on the data grid

1. In VMware vCenter, in the Navigator, click **vCenter**.
2. Click **Datacenters** or **Clusters**.
3. On the Objects tab, select the specific datacenter or cluster for which you want to view host details.
4. On the Monitor tab, select the **Dell Datacenter/Cluster Information** → **Overview** tab, and view the details:

   NOTE: To display the full list of details, select a specific host from the data grid.

Datacenter/Cluster Information	Displays the following: – Datacenter/cluster name – The number of Dell managed hosts – Total Energy Consumption. This link takes you to the Power Monitoring page for this datacenter or cluster.
Hardware Resources	Displays the following: – Total Processors This link takes you to the Processor Details page. – Total Memory This link takes you to the Memory Details page for this datacenter or cluster. – Virtual Disk Capacity This link takes you to the Virtual Disk page for this datacenter or cluster.
Warranty Summary	Displays the warranty status for the selected host. Status options include: – Expired warranty – Active warranty – Unknown warranty The link takes you to the Warranty Summary page.
Host	Displays the host name.
Service Tag	Displays the host Service Tag.
Model	Displays the Dell PowerEdge model.

Asset Tag	Displays the Asset Tag, if configured.
Chassis Service Tag	Displays the chassis Service Tag, if applicable.
OS Version	Displays the ESXi or ESX OS version.
Location	Blades only: Location displays the slot location. Otherwise Location displays, “Not Applicable.”
iDRAC IP	Displays the iDRAC IP address.
Service Console IP	Displays the Service Console IP.
CMC URL	Blades only: The CMC URL is the Chassis URL. Otherwise it displays, “Not Applicable.”
CPUs	Displays the number of CPUs.
Memory	Displays the host memory.
Power State	Displays if the host has power.
Last Inventory	Displays the day, date and time of last inventory job.
Connection Profile	Displays the name of the connection profile.
Remote Access Card Version	Displays the remote access card version.
BIOS Firmware Version	Displays the BIOS firmware version.

29

Viewing Hardware: FRUs for Datacenters or Clusters

View the Field Replaceable Unit (FRU) details for a datacenter or cluster on the Dell Datacenter/Cluster Information tab. For information to appear on this page, you must run an inventory job. Datacenter and cluster pages let you export information to a CSV file and offer filter/search functionality on the data grid. The data you view may vary depending on which view you are accessing the data. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

1. In VMware vCenter, in the Navigator, click **vCenter**.
2. Click **Datacenters** or **Clusters**.
3. On the Object tab, select the specific datacenter or cluster for which you want to view Hardware: FRU details.
4. On the Monitor tab, select the **Dell Datacenter/Cluster Information** tab, and on the **Hardware: FRU** sub-tab, view the following:

Host	Displays the host name.
Service Tag	Displays the Service Tag.
Part Name	Displays the FRU part name.
Part Number	Displays the FRU part number.
Manufacturer	Displays the manufacturer's name.
Serial Number	Displays the Manufacturer's serial number.
Manufacture Date	Displays the manufacture date.

30

Viewing Hardware: Processor Details for Datacenters or Clusters

View the processor details for a datacenter or cluster on the Dell Datacenter/Cluster Information tab. For information to appear on this page, you must run an inventory job. Datacenter and cluster pages let you export information to a CSV file and offers filter/search functionality on the data grid. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

1. In VMware vCenter, in the Navigator, click **vCenter**.
2. Click **Datacenters** or **Clusters**.
3. On the Datacenter or Cluster tab, select the specific datacenter or cluster for which you want to view Processor details.
4. On the Monitor tab, select the **Dell Datacenter/Cluster Information** tab, and on the Hardware: Processor sub-tab, view the following:

Host	Displays the host name.
Service Tag	Displays the Service Tag.
Socket	Displays the slot number.
Speed	Displays the current speed.
Brand	Displays the processor brand.
Version	Displays the processor version.
Cores	Displays the number of cores in this processor.

31

Viewing Hardware: Power Supply Details for Datacenters and Clusters

View the virtual power supply details for a datacenter or cluster on the Dell Datacenter or Cluster Information tab. For information to appear on this page, you must run an inventory job. Datacenter and cluster pages let you export information to a CSV file and offers filter/search functionality on the data grid. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

1. In VMware vCenter, in the Navigator, click **vCenter**.
2. Click **Datacenters** or **Clusters**.
3. On the Objects tab, select the specific datacenter or cluster for which you want to view Hardware: Power Supply details.
4. On the Monitor tab, select the **Dell Datacenter/Cluster Information** tab, and on the **Hardware: Power Supply** sub-tab, view the following:

Host	Displays the name of the host.
Service Tag	Displays the Service Tag.
Type	Displays the type of power supply. Power supply types include: – UNKNOWN – LINEAR – SWITCHING – BATTERY – UPS – CONVERTER – REGULATOR – AC – DC – VRM
Location	Displays the location of the power supply, such as Slot 1.
Output (Watts)	Displays the power in Watts.
Status	Displays the status of the power supply. The status options include: – OTHER – UNKNOWN – OK – CRITICAL – NOT CRITICAL – RECOVERABLE

- NOT RECOVERABLE
- HIGH
- LOW

32

Viewing Hardware: Memory Details for Datacenters and Clusters

View the memory details for a datacenter or cluster on the Dell Datacenter/Cluster Information tab. For information to appear on this page, you must run an inventory job. Datacenter and cluster pages let you export information to a CSV file and offers filter/search functionality on the data grid. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

1. In VMware vCenter, in the Navigator, click **vCenter**.
2. Click **Datacenters** or **Clusters**.
3. On the Objects tab, select the specific datacenter or cluster for which you want to view Hardware: Memory details.
4. On the Monitor tab, select the **Dell Datacenter/Cluster Information** tab, and on the **Hardware: Memory** sub-tab, view the following:

Host	Displays the host name.
Service Tag	Displays the Service Tag.
Slot	Displays the DIMM slot.
Size	Displays the memory size.
Type	Displays the memory type.

33

Viewing Hardware: NICs Details for Datacenters and Clusters

View the Network Interface Card (NIC) details for a datacenter or cluster on the Dell Datacenter/Cluster Information tab. For information to appear on this page, you must run an inventory job. Datacenter and cluster pages let you export information to a CSV file and offers filter/search functionality on the data grid. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

1. In VMware vCenter, in the Navigator, click **vCenter**.
2. Click **Datacenters** or **Clusters**.
3. On the Objects tab, select the specific datacenter or cluster for which you want to view Hardware: NICs details.
4. On the Monitor tab, select the **Dell Datacenter/Clusters Information** tab, and on the **Hardware: NICs** sub-tab, view the following:

Host	Displays the host name.
Service Tag	Displays the Service Tag.
Name	Displays the NIC name.
Manufacturer	Displays only the manufacturer name.
Mac Address	Displays the NIC mac address.

34

Viewing Hardware: PCI Slot Details for Datacenters and Clusters

View the PCI slot details for a datacenter or cluster on the Dell Datacenter/Cluster Information tab. For information to appear on this page, you must run an inventory job. Datacenter and cluster pages let you export information to a CSV file and offers filter/search functionality on the data grid. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

1. In VMware vCenter, in the Navigator, click **vCenter**.
2. Click **Datacenters** or **Clusters**.
3. On the Objects tab, select the specific datacenter or cluster for which you want to view Hardware: PCI Slot details.
4. On the Monitor tab, select the **Dell Datacenter/Cluster Information** tab, and on the **Hardware: PCI Slots** sub-tab, view the following:

Host	Displays the host name.
Service Tag	Displays the Service Tag.
Slot	Displays the slot.
Manufacturer	Displays the manufacturer name of the PCI slot.
Description	Displays the description of the PCI device.
Type	Displays the PCI slot type.
Width	Displays the data bus width, if available.

35
Viewing Hardware: Remote Access Card Details

View the Remote Access Card details for a datacenter or cluster on the Dell Datacenter/Cluster Information tab. For information to appear on this page, you must run an inventory job. Datacenter and cluster pages let you export information to a CSV file and offers filter/search functionality on the data grid. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

1. In VMware vCenter, in the Navigator, click **vCenter**.
2. Click **Datacenters** or **Clusters**.
3. On the Objects tab, select the specific datacenter or cluster for which you want to view Hardware: Remote Access Card details.
4. On the Monitor tab, select the **Dell Datacenter/Cluster Information** tab, and on the **Hardware: Remote Access Card** sub-tab, view the following:

Host	Displays the host name.
Service Tag	Displays the Service Tag.
IP Address	Display the IP address for the remote access card.
Mac Address	Displays the Mac address for the remote access card.
RAC Type	Displays the type of the remote access card.
URL	Displays the live URL for the iDRAC associated with this host.

36

Viewing Storage: Physical Disks for Datacenters and Clusters

View the physical storage details for a datacenter or cluster on the Dell Datacenter/Cluster Information tab. For information to appear on this page, you must run an inventory job. Datacenter and cluster pages let you export information to a CSV file and offers filter/search functionality on the data grid. See Running an Inventory Job Now.

NOTE: Hardware views are directly reporting the data from OMSA and iDRAC.

1. In VMware vCenter, in the Navigator, click **vCenter**.
2. Click **Datacenters** or **Clusters**.
3. On the Objects tab, select the specific datacenter or cluster for which you want to view Storage: Physical Disk details.
4. On the Monitor tab, select the **Dell Datacenter/Cluster Information** tab, and on the **Storage: Physical Disk** sub-tab, view the following:

   NOTE: To display the full list of details, select a specific host from the data grid.

Host	Displays the name of the host.
Service Tag	Displays the Service Tag.
Capacity	Displays the physical disk capacity.
Disk Status	Displays physical disk status. Options include: – ONLINE – READY – DEGRADED – FAILED – OFFLINE – REBUILDING – INCOMPATIBLE – REMOVED – CLEARED – SMART ALERT DETECTED – UNKNOWN – FOREIGN – UNSUPPORTED **NOTE:** For more information about the meaning of these alerts, see the *Dell OpenManage™ Server Administrator Storage Management User's Guide*, located at: http://support.dell.com/support/edocs/software/svradmin/5.1/en/omss_ug/html/adprin.html.
Model Number	Displays the model number of the physical storage disk.

Host	Displays the host name.
Last Inventory	Displays the day, month, and time of the last inventory that was run.
Status	Displays the host status.
Controller ID	Displays the controller ID.
Connector ID	Displays the connector ID.
Enclosure ID	Displays the enclosure ID.
Device ID	Displays the device ID.
Bus Protocol	Displays the bus protocol.
Hot Spare Type	Shows the hot spare type. Options include: – No No means there is no hot spare. – Global A global hot spare is an unused backup disk that is part of the disk group. – Dedicated A dedicated hot spare is an unused backup disk that is assigned to a single virtual disk. When a physical disk in the virtual disk fails, the hot spare is activated to replace the failed physical disk without interrupting the system or requiring your intervention.
Part Number	Displays the storage part number.
Serial Number	Displays the storage serial number.
Vendor Name	Displays the storage vendor name.

37

Viewing Storage: Virtual Disk Details for Datacenters and Clusters

View the virtual storage details for a datacenter or cluster on the Dell Datacenter/Cluster tab. For information to appear on this page, you must run an inventory job. The data you view may vary depending on which view you are accessing the data. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now. Datacenter and cluster pages let you export information to a CSV file and offers filter/search functionality on the data grid.

1. In VMware vCenter, in the Navigator, click **vCenter**.
2. Click **Datacenters** or **Clusters**.
3. On the Objects tab, select the specific datacenter or cluster for which you want to view Storage: Virtual Disk details.
4. On the Monitor tab, select the **Dell Datacenter/Cluster Information** tab, and on the Storage: Virtual Disk sub-tab, view the following:

   NOTE: To display the full list of details, select a specific host from the data grid.

Host	Displays the name of the host.
Service Tag	Displays the Service Tag.
Name	Displays the name of the virtual disk.
Physical Disk	Displays on which physical disk the virtual disk is located.
Capacity	Displays the capacity of the virtual disk.
Layout	Displays the layout type of the virtual storage. This means the type of RAID that was configured for this virtual disk.
Host	Displays the host name.
Name	Displays the virtual disk name.
Last Inventory	Displays the day, date and time the inventory was last run.
Controller ID	Displays the controller ID.
Device ID	Displays the device ID.
Media Type	Displays either SSD or HDD.
Bus Protocol	This displays the technology that the physical disks included in the virtual disk are using. Possible values are: – SCSI – SAS – SATA

Stripe Size The stripe size refers to the amount of space that each stripe consumes on a single disk.

Default Read Policy The default read policy supported by the controller. Options include:

- Read-Ahead
- No-Read-Ahead
- Adaptive Read-Ahead
- Read Cache Enabled
- Read Cache Disabled

Default Write Policy The default write policy supported by the controller. Options include:

- Write-Back
- Force Write Back
- Write Back Enabled
- Write-Through
- Write Cache Enabled Protected
- Write Cache Disabled

Disk Cache Policy The default cache policy supported by the controller. Options include:

- Enabled
  This means cache I/O.
- Disabled
  This means direct I/O.

38

Viewing Firmware Details for Datacenters and Clusters

View the firmware details for datacenters or clusters on the Dell Host tab. For information to appear on this page, you must run an inventory job. Datacenter and cluster pages let you export information to a CSV file and offers filter/search functionality on the data grid. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

1. In VMware vCenter, in the Navigator, click **vCenter**.
2. Click **Datacenters** or **Clusters**.
3. On the Objects tab, select the specific datacenter or cluster for which you want to view firmware details.
4. On the Monitor tab, select the **Dell Datacenter/Cluster Information** tab, and on the Firmware sub-tab, view the following:

Host	Displays the name of the host.
Service Tag	Displays the Service Tag.
Name	Displays the name of all the firmware on this host.
Version	Displays the version of all the firmware on this host.

39

Viewing Warranty Summary Details for Datacenters and Clusters

You must have run a warranty job to view a warranty summary. See Running a Warranty Job Now.

View the warranty summary details for a datacenter or cluster on the Dell Datacenter/Cluster Information tab. Datacenter and cluster pages let you export information to a CSV file and offers filter/search functionality on the data grid. The Warranty Summary page lets you monitor the warranty expiration date. Warranty settings control when server warranty information is retrieved from Dell online by enabling or disabling the warranty schedule and then setting the Minimum Days Threshold alert. See Warranty History.

1. In VMware vCenter, in the Navigator, click **vCenter**.
2. Click **Datacenters** or **Clusters**.
3. On the Objects tab, select the specific datacenter or cluster for which you want to view warranty summary details.
4. On the Monitor tab, select the **Dell Datacenter/Cluster Information** tab, and on Warranty Summary sub-tab, view the following:

Warranty Summary	The host warranty summary is displayed using icons to visually show the number of hosts in each status category.
Host	Displays the name of the host.
Service Tag	Displays the Service Tag for the host.
Description	Displays a description.
Warranty Status	Displays the warranty status of the host. Status options include: – Active The host is under warranty, and has not exceeded any threshold. – Warning The host is Active, but exceeded the warning threshold. – Critical Same as warning, but for a critical threshold. – Expired The warranty has expired for this host. – Unknown OpenManage Integration for VMware vCentercannot get warranty status because the warranty job has not run, an error has occurred getting the data, or the system does not have a warranty.
Days Left	Displays the number of days left for the warranty.

40

Viewing Power Monitoring for Datacenters and Clusters

View the power monitoring details for a datacenter or cluster on the Dell Datacenter/Cluster Information tab. For information to appear on this page, you must run an inventory job. Datacenter and cluster pages let you export information to a CVS file and offers filter/search functionality on the data grid. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

1. In VMware vCenter, in the Navigator, click **vCenter**.
2. Click **Datacenters** or **Clusters**.
3. On the Objects tab, select the specific datacenter or cluster for which you want to view power monitoring details.
4. On the Monitor tab, select the **Dell Datacenter/Cluster Information Host** tab, and on the Power Monitoring sub-tab, view the following:

   NOTE: To display the full list of details, select a specific host from the data grid.

Host	Displays the name of the host.
Service Tag	Displays the Service Tag.
Current Profile	Displays power profile to maximize your system's performance and conserve energy.
Energy Consumption	Displays the energy consumption of the host.
Peak Reserve Capacity	Displays the peak power reserve capacity.
Power Budget	Displays the power cap for this host.
Warning Threshold	Displays your system's configure maximum value for temperature probe warning threshold.
Failure Threshold	Displays your system's configure maximum value for temperature probe failure threshold.
Instant Reserve Capacity	Displays the host instantaneous headroom capacity.
Energy Consumption Start Date	Displays the date and time when the host began to consume power.
Energy Consumption End Date	Displays the date and time when the host stopped to consume power.
System Peak Power	Displays the host peak power.
System Peak Power Start Date	Displays the date and time when the host peak power began.
System Peak Power End Date	Displays the date and time when the host peak power ended.

System Peak Amps	Displays the hosts peak Amps.
System Peak Amps Start Date	Displays the beginning date and time of the host peak amps.
System Peak Amps End Date	Displays the end date and time of the host peak amps.

41

Troubleshooting

Use this section to find answers to troubleshooting questions. This section includes:

- Frequently asked questions (FAQ)
- Bare metal deployment issues
- Contacting Dell
- Related product information

Frequently Asked Questions (FAQ)

This section contains some common questions and solutions.

'Settings' page fails to load, if we navigate away and go back to 'Settings' page.

In the Web Client, if you navigate away and go back to the 'Settings' page, sometimes the page fails to load and the spinner continues to show. This is a refresh issue and the page is not getting refreshed correctly.

Resolution: Click the global refresh and the screen will refresh correctly.

Versions Affected: 2.0

Why is the DNS configuration settings restored to original settings after appliance reboot if using DHCP for appliance IP and DNS settings overwritten

There is a known defect where statically assigned DNS settings are replaced by values from DHCP. This can happen when DHCP is used to obtain IP settings, and DNS values are assigned statically. When the DHCP lease is renewed or the appliance is restarted the statically assigned DNS settings are removed. Resolution: Statically assign IP settings when the DNS server settings will be different from DHCP.

Version Affected: All

Using OpenManage Integration for VMware vCenter to update an Intel Network card with the firmware version of 13.5.2 is not supported.

There is a known issue with Dell PowerEdge 12th generation servers and some Intel Network cards with the firmware version of 13.5.2. Updating some models of Intel network cards at this version of firmware fails when the firmware update is applied using the Lifecycle Controller. Customers with this version of firmware must update the network driver software using an operating system. If the Intel Network card has a version of firmware other than 13.5.2, you can update using OpenManage Integration for VMware vCenter. For more information, see http://en.community.dell.com/techcenter/b/techcenter/archive/2013/03/20/intel-network-controller-card-with-v13-5-2-firmware-cannot-be-upgraded-using-lifecycle-controller-to-v13-5-6.aspx

NOTE: Note: When using the one-to-many firmware update, avoid selecting Intel network adapters that are at version 13.5.2, as the update will fail and stop the update task from updating remaining servers.

On trying a firmware update with an invalid DUP, the hardware update job status on the vCenter console neither fails nor times-out for hours, though the job status in LC says 'FAILED'. Why is this happening?

When the invalid DUP is picked for firmware update, the status of the task in the vCenter console window remains 'In Progress' but the message is changed to the reason of failure. This is a known VMWare defect and will be fixed in the future releases of VMWare vCenter.

Resolution: The task has to be cancelled manually.

Version Affected: All

Administration Portal is still showing the unreachable Update Repository location.

If the user provided a unreachable Update Repository path, the error message "Failed: Error while connecting to the URL …. " is displayed on the top of the Appliance Update view, however the Update Repository Path is not cleared out to the value before update.

Resolution: Move out of this page to another page and make sure the page is refreshed.

Version Affected: All

Why do I see "Task cannot be scheduled for the time in the past" error in inventory schedule/Warranty schedule page of Initial Configuration Wizard

In the Web Client, if the user picks 'All registered vCenters' in the Initial Configuration wizard, and if there are some vCenters with no hosts or vCenters where some have Inventory or Warranty task already scheduled and some with no Inventory or Warranty schedule set yet, then the user will sometimes see an error "Task cannot be scheduled for the time in the past".

Resolution: If you have situations where there are some vCenters with no hosts or vCenters where some have Inventory or Warranty task already scheduled and some with no Inventory or Warranty schedule set yet, run the setting of Inventory and Warranty schedule separately again from the Settings page for those vCenters.

Versions Affected: 2.0

Why did my system not enter maintenance mode when I performed a one-to-many firmware update?

Some firmware updates do not require rebooting the host. In that case, the firmware update is performed without putting the host into maintenance mode.

Warranty and Inventory schedule for all Vcenters is not applying when selected under "Dell Home > Monitor > Job Queue > Warranty/Inventory History >Schedule"

A customer navigates to the job queue page, selects a vCenter and selects the modify schedule button. When the dialog comes up, they see a checkbox that says apply this new setting to all registered vCenters. When they select this and press Apply, it only applies the setting to the particular vCenter they initially selected and not all vCenters. The 'Apply to All Registered vCenters' is not applicable when Warranty or Inventory schedule is modified from the Job Queue page.

Resolution: Use the modify Warranty or Inventory schedule from the Job Queue only to modify the selected vCenter.

Versions Affected: 2.0

Why is the Installation date showing up as 12/31/1969 for some of the firmware on the firmware page.

In the Web Client, the installation date is showing up as 12/31/1969 for some firmware items on the firmware page for a host. If the firmware installation date is not available, then this very old date is shown.

Resolution: If you see this old date for any firmware component, consider that the installation date is not available for it.

Versions Affected: 2.0

Why is successive Global refresh cause exception to be thrown in Recent Task window

If a customer tries to press the refresh button repeatedly, the VMware UI may throw an exception.

Resolution: User should dismiss this error and can continue on.

Version Affected: 2.0

Why is the Web client UI distorted for few of the Dell screens in IE 10

In some cases, when a popup dialog is presented, the data in the background may turn completely white and be distorted.

Resolution: Close the dialog, the screen will return back to normal.

Version Affected: 2.0

Even if my repository has bundles for selected 11G system, why is firmware update showing that I have no bundles for Firmware Update?

When I added a host to the connection profile in lockdown mode, the inventory kicked off but failed stating that "No Remote Access Controller was found or Inventory is not supported on this host." Inventory is supposed to work for a host in lockdown mode, right?

If you put the host in lockdown mode or remove a host from lockdown mode, you must wait 30–minutes before performing the next operation on the If I pick a 11G host for firmware update, the firmware update wizard will not show any bundles even if the repository provided has bundles for that system. This will happen because the 11G host might not configured for OMSA to send traps to OpenManage Integration.

Resolution: Ensure that the host is compliant using the host Compliance screen of OpenManage Integration .NET client. If it is not compliant, use the fix Host Compliance to get it compliant.

Version Affected: 2.0

Why am I not seeing the OpenManage Integration Icon on the Web Client even if the registration of the plug-in to the vCenter was successful?

Dell OpenManage Integration Plug-in icon is not displayed on the Web client unless the vCenter Web Client services are restarted or the Box is rebooted. When a user registers the OpenManage Integration for VMware vCenter appliance, it registers with both the .Net client and the Web client. If a user unregisters the appliance and then either reregisters the same version or registers a new version of the appliance, it will successfully register with both clients, but the Dell icon may not appear in the Web Client. This is due to a caching issue from VMware. To clear the issue, a user needs to restart the Web Client Service on the vCenter Server. Only then will the plug-in appear in the UI.

Resolution: Restart the Web Client Service on the vCenter Server.

Version Affected: 2.0

I get an exception whenever I click finish after editing a connection profile through Web Client. Why?

This happens when the vCenter server is registered to the appliance through IP instead of FQDN. The connection profile can be edited through the .net client. Re-registering the vCenter server to the same appliance will not solve this. A new setup registered with FQDN is required.

I am unable to see the connection profiles to which a host belongs to when I create\edit a connection profile in web GUI. Why?

This happens when the vCenter server is registered to the appliance through IP instead of FQDN. Re-registering the vCenter server to the same appliance will not solve this. A new setup registered with FQDN is required.

On editing a Connection profile the select host window in the Web UI is blank. Why?

This happens when the vCenter server is registered to the appliance through IP instead of FQDN. Re-registering the vCenter server to the same appliance will not solve this . A new setup registered with FQDN is required.

How Come I See An Error Message Displayed After Clicking The Firmware Link?

If you have a slow network speed (9600BPS), you may get a Communication Error Message. This error message may display when you click the Firmware link in the vSphere Client for the OpenManage Integration for VMware vCenter. It happens when the connection times out while trying to obtain the Software Inventory list. Microsoft Internet Explorer initiates this timeout. For Microsoft Internet Explorer versions 9/10, the default “Receive Time out” value is set to 10 seconds. Fix this issue by using the following steps.

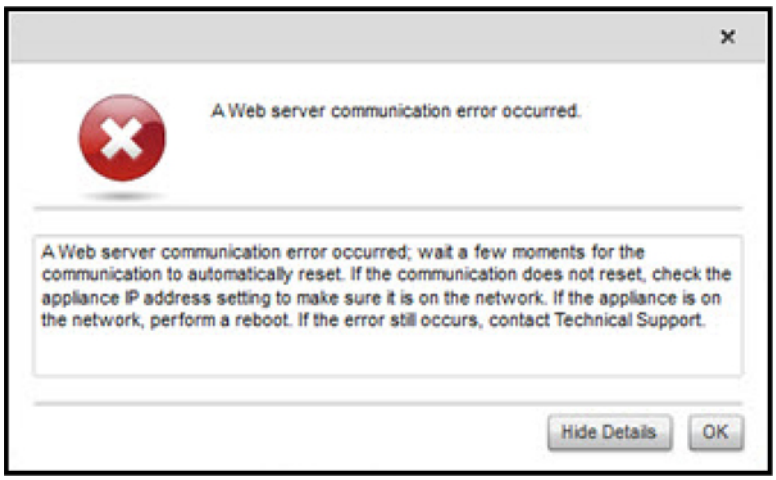
A Web server communication error occurred.
A Web server communication error occurred; wait a few moments for the communication to automatically reset. If the communication does not reset, check the appliance IP address setting to make sure it is on the network. If the appliance is on the network, perform a reboot. If the error still occurs, contact Technical Support.
Hide Details
OK

Figure 1. Firmware link communication error

1. Open Microsoft Registry Editor (Regedit).
2. Navigate to the following location:
   KHEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
3. Add a DWORD value for ReceiveTimeout.
4. Set the value to 30 seconds (30000) [This value may need to be a higher value in your environment].
5. Exit Regedit.
6. Restart Internet Explorer.

NOTE: Just opening a new Internet Explorer window is not enough. Restart the Internet Explorer browser.

What generation of Dell servers does the OpenManage Integration for VMware vCenter configure and support for SNMP traps?

OpenManage Integration for VMware vCenter supports OMSA SNMP traps on pre-12th generation servers and iDRAC traps on 12th generation servers.

What vCenters in linked mode are managed by OpenManage Integration for VMware vCenter?

OpenManage Integration for VMware vCenter manages only registered vCenters in linked mode.

Does OpenManage Integration for VMware vCenter support vCenter in linked mode?

Yes , OpenManage Integration for VMware vCenter supports up to 10 vCenters in linked mode. For more information on how OpenManage Integration for VMware vCenter working in linked mode see the white paper, *OpenManage Integration for VMware vCenter for VMware vCenter: Working in Linked Mode* on www.Dell.com.

What are the Required Port Settings for the OpenManage Integration for VMware vCenter?

NOTE: When deploying the OMSA agent using the *Fix non-complient vSphere hosts* link available from the Compliance window in the Dell Management Center, the OpenManage Integration for VMware vCenter starts the httpClient service and enables port 8080 on releases after ESXI 5.0 to download OMSA VIB and install it. Once the OMSA installation is completed the service automatically stops and the port is closed.

Use these port settings for the OpenManage Integration for VMware vCenter.

Table 3. Virtual Appliance Ports

Port Number	Protocols	Port Type	Max. Encryption Level	Direction	Usage	Configurable
21	FTP	TCP	None	Out	FTP command client	No
53	DNS	TCP	None	Out	DNS client	No
80	HTTP	TCP	None	Out	Dell Online Data Access	No
80	HTTP	TCP	None	In	Administration Console	No
162	SNMP Agent	UDP	None	In	SNMP Agent (server)	No
11620	SNMP Agent	UDP	None	In	SNMP Agent (server)	No
443	HTTPS	TCP	128–bit	In	HTTPS server	No
443	WSMAN	TCP	128–bit	In/Out	iDRAC/OMSA communication	No
4433	HTTPS	TCP	128–bit	In	Auto Discovery	No

Port Number	Protocols	Port Type	Max. Encryption Level	Direction	Usage	Configurable
2049	NFS	UDP	None	All	Public Share	No
4001–4004	NFS	UDP	None	All	Public Share	No
11620	SNMP Agent	UDP	None	Om	SNMP Agent (server)	No

Table 4. Managed Nodes

Port Number	Protocols	Port Type	Max. Encryption Level	Direction	Usage	Configurable
162, 11620	SNMP	UDP	None	Out	Hardware events	No
443	WSMAN	TCP	128–bit	In	iDRAC/OMSA communication	No
4433	HTTPS	TCP	128–bit	Out	Auto Discovery	No
2049	NFS	UDP	None	All	Public Share	No
4001–4004	NFS	UDP	None	All	Public Share	No
443	HTTPS	TCP	128–bit	In	HTTPS server	No
8080	HTTP	TCP		In	HTTP server; downloads the OMSA VIB and fixes non-compliant vSphere hosts	No
50	RMCP	UDP/TCP	128–bit	Out	Remote Mail Check Protocol	No
51	IMP	UDP/TCP	N/A	N/A	IMP Logical Address Maintenance	No
5353	mDNS	UDP/TCP		All	Multicast DNS	No
631	IPP	UDP/TCP	None	Out	Internet Printing Protocol (IPP)	No
69	TFTP	UDP	128–bit	All	Trivial File Transfer	No
111	NFS	UDP/TCP	128–bit	In	SUN Remote Procedure Call (Portmap)	No
68	BOOTP	UDP	None	Out	Bootstrap Protocol Client	No

What are the Minimum requirements for successful installation and operation of the virtual appliance?

The following settings outline the minimum appliance requirements:

- Physical RAM: 3 GB.
- Reserved Memory: 1 GB

  NOTE: For optimal performance Dell recommends 3 GB.
- Disk: 32.5 GB.
- CPU: 2 virtual CPUs.

How Do I Find the Expected Translations for Renewing Warranty?

When you click on the Renew Warranty button, the Web page may display in English or in the local language where the server is physically located. The tables below illustrate the expected translations:

Table 5. Expected translations.

	Client location	Service Tag location	Does OpenManage Integration for VMware vCenter support client locale?	Can OpenManage Integration for VMware vCenter show pages in client locale language?	OpenManage Integration for VMware vCenter shows pages in default English
1	Location A	Location A	Yes	Yes	No
2	Location A	Location B	No	No	Yes
3	Location A	Location B	Yes	No	Yes
4	Location A	Location B	Yes	No	Yes
5	Location A	Location A	No	No	Yes

Use this following example.

Table 6. Example

	Client location	Service Tag location	Does OpenManage Integration for VMware vCenter support client locale?	Can OpenManage Integration for VMware vCenter show pages in client locale language?	OpenManage Integration for VMware vCenter shows pages in default English
1	France	France	Yes	Yes	No
2	Brazil	China	No	No	Yes
3	Germany	China	Yes	No	Yes
4	China	Brazil	Yes	No	Yes
5	India	India	No	No	Yes

How come I do not see my new iDRAC version details listed on the vCenter Hosts & Clusters page?

After the successful completion of a firmware update task in the vSphere Web client's recent tasks pane, refresh the Firmware Update page and verify the firmware versions. If the page shows the old versions, then go to Host Compliance page in Dell Management Center and check the CISOR status of that host. If CISOR is not enabled, then enable CISOR

and reboot host. If the CISOR was already enabled, then login to the iDRAC console, reset iDRAC, wait for few minutes, and then refresh the Firmware Update page in vSphere Web client.

NOTE: The host compliance is not available in the web client and you would have to use the host compliance feature from the vSphere .Net client

How Do I Test Event Settings by Using OMSA to Simulate a Temperature Hardware Fault?

To make sure that events are functioning correctly:

1. In the OMSA user interface, navigate to **Alert Management** → **Platform Events** .
2. Select the **Enable Platform Event Filter Alerts** check box.
3. Scroll down to the bottom, and click **Apply Changes**.
4. To make sure that a specific event is enabled, such as temperature warning, from the tree on the left, select **Main System Chassis**.
5. Under **Main System Chassis**, select **Temperatures**.
6. Select the **Alert Management** tab, and select **Temperature Probe Warning**.
7. Select the **Broadcast a Message** check box, and select **Apply Changes**.
8. To cause the temperature warning event, from the tree view on the left, select **Main System Chassis**.
9. Select **Temperatures** under **Main System Chassis**.
10. Select the **System Board Ambient Temp** link, and select the **Set to Values** option button.
11. Set the **Maximum Warning Threshold** to below the current listed reading; for example if the current reading is 27, set the threshold to **25**.
12. Select **Apply Changes**, and the temperature warning event is generated. To cause another event, restore the original settings using the same **Set to Values** option. Events are generated as warnings, and then to a normal state. If everything is working properly, navigate to the **vCenter Tasks & Events** view; a temperature probe warning event should be displayed.

    NOTE: There is a filter for duplicate events; if you try to trigger the same event too many times in a row, you will only receive one event. Allow at least 30 seconds between events to see all events.

I Have the OMSA Agent Installed on a Dell Host System, But I Still Get an Error Message That OMSA is Not Installed. What Should I Do?

To resolve this issue on an 11th generation server:

1. Install **OMSA** with the **Remote Enablement** component on the host system.
2. If you are using the command line to install OMSA, make sure to specify the **-c option**. If OMSA is already installed, reinstall it with the -c option and restart the service:

   ```
   srvadmin-install.sh -c
   srvadmin-services.sh restart
   ```

   For an ESXi host, you must install **OMSA VIB** using the **VMware Remote CLI tool**, and reboot the system.

Can the OpenManage Integration for VMware vCenter Support ESX/ESXI with Lockdown Mode Enabled?

Yes. Lockdown Mode is supported in this release on hosts ESXi 4.1 and above.

Inventory is Failing on Hosts ESXi 4.0 Update2 and ESXi Update 3 in Lockdown Mode after a Reboot.

Lockdown Mode requires ESXi 4.1 or later. If you are using an earlier ESXi version, when a host is rebooted for any reason during Lockdown Mode, inventory continues failing unless you perform the following steps on host after a reboot.

The workaround steps for ESXi 4.0 Update2 and Update3 are:

1. In **vSphere Web Client**, select **Hosts and Clusters**, then in the left pane, select the **host** and then click the **Configuration** tab.
2. In the left pane, under **Software** click **Security Profile**.
3. Scroll down to **Lockdown Mode**, and then click **Edit**.
4. In the **Lockdown Mode** dialog box, to disable Lockdown Mode, clear the **Enable** check box, and then click **OK**.
5. Log in to the host console and select **Restart Management Agents**, press **<ENTER>**, and to confirm, press **<F11>**.
6. To enable Lockdown Mode, repeat steps 1 through 4, except this time select the **Enable** check box, and then click **OK**.

When I tried to use lockdown mode, it failed.

When I added a host to the connection profile in lockdown mode, the inventory kicked off but failed stating that "No Remote Access Controller was found or Inventory is not supported on this host." Inventory is supposed to work for a host in lockdown mode, right?

If you put the host in lockdown mode or remove a host from lockdown mode, you must wait 30–minutes before performing the next operation on the OpenManage Integration for VMware vCenter.

What Setting Should I Use For UserVars.CIMoeMProviderEnable With ESXi 4.1 U1?

Set **UserVars.CIMoemProviderEnabled** to 1.

I Am Using A Reference Server to Create a Hardware Profile But it Failed. What Should I Do?

Check to make sure that minimum recommended versions of iDRAC firmware, Lifecycle Controller firmware, and BIOS are installed.

To make sure that the data retrieved from the reference server is current, enable **Collect System Inventory On Restart (CSIOR)**, and restart the reference server prior to extraction of data.

I Am Attempting to Deploy ESX/ESXi on a Blade Server and it Failed. What Should I Do?

1. Make sure the **ISO location (NFS path)** and staging **folder paths** are accurate.
2. Make sure the **NIC** selected during assignment of server identity is on the same network as the virtual appliance.
3. If using **static IP address**, make sure the network information provided (including subnet mask and default gateway) is accurate. In addition, , make sure the IPaddress is not already assigned on the network.
4. Make sure at least one **Virtual Disk** is seen by the system. ESXi also installs to an internal RIPS SD card.

Why are My Hypervisor Deployments Failing on my Dell PowerEdge R210 II Machines?

A timeout issue on Dell PowerEdge R210 II systems produces a hypervisor deployment failure error due to the failure of the BIOS to boot from the attached ISO. To resolve this issue, manually install hypervisor on the machine.

Why Do I See Auto-discovered Systems Without Model Information in the Deployment Wizard

This usually indicates that the firmware version installed on the system does not meet recommended minimum requirements. In some cases, a firmware update may not have registered on the system. Cold booting the system or reseating the blade fixes this problem. The newly enabled account on the iDRAC must be disabled and auto-discovery reinitiated to provide model information and NIC information to the OpenManage Integration for VMware vCenter.

The NFS Share is Set Up With the ESX/ESXI ISO, but Deployment Fails with Errors Mounting the Share Location.

To find the solution:

1. Make sure the iDRAC is able to ping the appliance.
2. Make sure your network is not running too slow.

How Do I Force Removal of the Virtual Appliance?

1. Go to **https://<vcenter_serverIPAddress>/mob**
2. Click **Content.**
3. Click **ExtensionManager**.
4. Click **UnregisterExtension**.
5. Enter the extension key to unregister com.dell.plugin.OpenManage Integration for VMware vCenter, then click **Invoke method**.
6. In the vSphere Web client, power off the OpenManage Integration for VMware vCenter and delete it. The key to unregsiter must be for the Web Client.

Entering a Password in the Backup Now Screen Receives an Error Message

If you are using a low resolution monitor, the Encryption Password field is not visible from the BACKUP NOW window. You must scroll down the page to enter the encryption password.

In the vSphere Web Client, Clicking the Dell Server Management Portlet Or the Dell Icon Returns A 404 Error.

Check if the appliance is running; if not, then restart it from the vSphere Web client. Wait for a few minutes for the virtual appliance Web service to start, and refresh the page. If the error continues, try and ping the appliance using the IP address or fully-qualified domain name from a command line. If the ping does not resolve, review your network settings to make sure they are correct.

My Firmware Update Failed. What Do I Do?

Check the virtual appliance logs to see if the tasks timed out. If so, iDRAC needs to be reset by performing a cold reboot. Once the system is up and running, check to see if the update was successful by either running an inventory or using the Firmware tab.

My vCenter Registration Failed. What Can I Do?

vCenter registration can fail due to communication issues, therefore if you are experiencing these issues one solution is to use a static IP address. To use a static IP address, in the Console tab of the OpenManage Integration for VMware vCenter and select **Configure Network** → **Edit Devices** and enter the correct **gateway** and **FQDN** (fully-qualified domain name). Enter the DNS server name under Edit DNS Config.

NOTE: Make sure that the virtual appliance can resolve the DNS server you entered.

Performance during Connection Profile Test Credentials is extremely slow or unresponsive.

The iDRAC on a server has only one user (for example, only *root*) and the user is in a disabled state, or all users are in a disabled state. Communicating to a server in a disabled state causes delays. To fix this issue, you can either fix the disable state of the server, or reset iDRAC on the server to re-enable the root user to default setting.

To fix a server in a disabled state:

1. Open the Chassis Management Controller console and select the disabled server.
2. To automatically open the iDRAC console, click **Launch iDRAC GUI**.
3. Navigate to the user list in iDRAC console, and choose one of the following:
   - iDRAC 6 : Select **iDRAC settings** → **Network/Security tab** → **Users tab.**
   - iDRAC 7 : Select **User authentication**.
4. To edit the settings, in the User ID column, click the link for the admin (root) user.
5. Click **Configure User**, and then click **Next**.
6. In the User Configuration page for the selected user, select the check box next to Enable user, and then and click **Apply**.

Does the OpenManage Integration for VMware vCenter support the VMware vCenter Server appliance?

Yes, the OpenManage Integration for VMware vCenter v2.0 supports the VMware vCenter Server appliance.

Does the OpenManage Integration for VMware vCenter support the vSphere Web Client?

Yes, the OpenManage Integration for VMware vCenter supports the VMware vSphere Web client.

Bare Metal Deployment Issues

This section deals with issues found during the deployment process. The v 2.0 does not support deployment from the web client, but is available only using the vSphere .Net client.

Auto-Discovery and Handshake Prerequisites

- Prior to running auto-discovery and handshake, make sure that iDRAC and Lifecycle Controller firmware and BIOS versions meet the minimum recommendations.
- CSIOR must have run at least once on the system or iDRAC.

Hardware Configuration Failure

- Before initiating a deployment task, make sure the system has completed CSIOR and is not in the process of rebooting.
- It is highly recommended that BIOS configuration be run in Clone mode, so that the reference server is an identical system.
- Some controllers do not allow creation of a RAID 0 array with one drive. This feature is supported only on high-end controllers, and the application of such a hardware profile can cause failures.

Contacting Dell

NOTE: If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell for sales, technical support, or customer service issues:

1. Visit **dell.com/support**
2. Select your support category.
3. Verify your country or region in the Choose a Country/Region drop-down menu at the top of page.
4. Select the appropriate service or support link based on your need.

Where To Get Additional Help For This Software

View or download Dell virtualization documentation: **http://support.dell.com/support/edocs/software/eslvmwre/**. Dell vCenter Plug-In Frequently Asked Questions **http://i.dell.com/sites/content/business/solutions/virtualization/en/Documents/dell-management-plugin-vmware-vcenter-faq.pdf**

OpenManage Integration for VMware vCenter Related Information

- View or download Dell server documentation for PowerEdge™ Servers at: http://www.dell.com/poweredgemanuals
- Dell OpenManage System Administrator documents http://www.dell.com/support/Manuals
- Dell Lifecycle Controller documentation http://www.dell.com/esmmanuals

42

Virtualization—Related Events

The following table contains the virtualization-related critical and warning events, including event name, description and severity level.

Event Name	Description	Severity	Recommended Action
Dell-Current sensor detected a warning value	A current sensor in the specified system exceeded its warning threshold.	Warning	No action
Dell-Current sensor detected a failure value	A current sensor in the specified system exceeded its failure threshold.	Error	Put the system into maintenance mode
Dell-Current sensor detected a non-recoverable value	A current sensor in the specified system detected an error from which it cannot recover	Error	No action
Dell-Redundancy regained	Sensor Returned to Normal Value	Info	No action
Dell-Redundancy degraded	A redundancy sensor in the specified system detected that one of the components of the redundancy unit has failed but the unit is still redundant.	Warning	No action
Dell - Redundancy lost	A redundancy sensor in the specified system detected that one of the components in the redundant unit has been disconnected, has failed, or is not present.	Error	Put the system into maintenance mode
Dell - Power supply returned to normal	Sensor Returned to Normal Value	Info	No action
Dell - Power supply detected a warning	A power supply sensor reading in the specified system exceeded a user definable warning threshold.	Warning	No action
Dell - Power supply detected a failure	A power supply has been disconnected or has failed.	Error	Put the system into maintenance mode

Dell - Power supply sensor detected a non-recoverable value	A power supply sensor in the specified system detected an error from which it cannot recover.	Error	No action
Dell - Memory Device Status warning	A memory device correction rate exceeded an acceptable value.	Warning	No action
Dell - Memory Device error	A memory device correction rate exceeded an acceptable value, a memory spare bank was activated, or a multibit ECC error occurred.	Error	Put the system into maintenance mode
Dell - Fan enclosure inserted into system	Sensor returned to normal value.	Info	No action
Dell - Fan enclosure removed from system	A fan enclosure has been removed from the specified system.	Warning	No action
Dell - Fan enclosure removed from system for an extended amount of time	A fan enclosure has been removed from the specified system for a user-definable length of time.	Error	No action
Dell - Fan enclosure sensor detected a non-recoverable value	A fan enclosure sensor in the specified system detected an error from which it cannot recover.	Error	No action
Dell - AC power has been restored	Sensor Returned to Normal Value.	Info	No action
Dell - AC power has been lost warning	An AC power cord has lost its power, but there is sufficient redundancy to classify this as a warning.	Warning	No action
Dell - An AC power cord has lost its power	An AC power cord has lost its power, and lack of redundancy requires this to be classified as an error.	Error	No action
Dell - Processor sensor returned to a normal value	Sensor Returned to Normal Value	Info	No action
Dell - Processor sensor detected a warning value	A processor sensor in the specified system is in a throttled state.	Warning	No action
Dell - Processor sensor detected a failure value	A processor sensor in the specified system is disabled, has a	Error	No action

	configuration error, or experienced a thermal trip.		
Dell - Processor sensor detected a non-recoverable value	A processor sensor in the specified system has failed.	Error	No action
Dell - Device configuration error	A configuration error was detected for a pluggable device in the specified system.	Error	No action
Dell - Battery sensor returned to a normal value	Sensor Returned to Normal Value	Info	No action
Dell - Battery sensor detected a warning value	A battery sensor in the specified system detected that a battery is in a predictive failure state.	Warning	No action
Dell - Battery sensor detected a failure value	A battery sensor in the specified system detected that a battery has failed.	Error	No action
Dell - Battery sensor detected a nonrecoverable value	A battery sensor in the specified system detected that a battery has failed.	Error	No Action
Dell - Thermal shutdown protection has been initiated	This message is generated when a system is configured for thermal shutdown due to an error event. If a temperature sensor reading exceeds the error threshold for which the system is configured, the operating system shuts down and the system powers off. This event may also be initiated on certain systems when a fan enclosure is removed from the system for an extended period of time.	Error	No action
Dell - Temperature sensor returned to a normal value	Sensor Returned to Normal Value.	Info	No action
Dell - Temperature sensor detected a warning value	A temperature sensor on the backplane board, system board, CPU, or drive carrier in the specified system exceeded its warning threshold.	Warning	No action

Dell - Temperature sensor detected a failure value	A temperature sensor on the backplane board, system board, or drive carrier in the specified system exceeded its failure threshold value.	Error	Put the system into maintenance mode
Dell - Temperature sensor detected a non-recoverable value	A temperature sensor on the backplane board, system board, or drive carrier in the specified system detected an error from which it cannot recover.	Error	No action
Dell - Fan sensor returned to a normal value	Sensor Returned to Normal Value	Info	No action
Dell - Fan sensor detected a warning value	Fan Sensor reading in the host <x> exceeded a warning threshold value.	Warning	No Action
Dell - Fan sensor detected a failure value	A fan sensor in the specified system detected the failure of one or more fans.	Error	Put the system into maintenance mode
Dell - Fan sensor detected a nonrecoverable value	A fan sensor detected an error from which it cannot recover.	Error	No action
Dell - Voltage sensor returned to a normal value	Sensor Returned to Normal Value	Info	No action
Dell - Voltage sensor detected a warning value	A voltage sensor in the specified system exceeded its warning threshold	Warning	No action
Dell - Voltage sensor detected a failure value	A voltage sensor in the specified system exceeded its failure threshold.	Error	Put the system into maintenance mode
Dell - Voltage sensor detected a nonrecoverable value	A voltage sensor in the specified system detected an error from which it cannot recover.	Error	No action
Dell - Current sensor returned to a normal value	Sensor Returned to Normal Value.	Info	No action
Dell - Storage: storage management error	Storage management has detected a device independent error condition.	Error	Put the system into maintenance mode

Dell - Storage: Controller warning	A portion of the physical disk is damaged.	Warning	No action
Dell - Storage: Controller failure	A portion of the physical disk is damaged	Error	Put the system into maintenance mode
Dell - Storage: Channel Failure	Channel failure.	Error	Put the system into maintenance mode
Dell - Storage: Enclosure hardware information	Enclosure hardware information.	Info	No action
Dell - Storage: Enclosure hardware warning	Enclosure hardware warning.	Warning	No action
Dell - Storage: Enclosure hardware failure	Enclosure hardware error.	Error	Put the system into maintenance mode
Dell - Storage: Array disk failure	Array disk failure.	Error	Put the system into maintenance mode
Dell - Storage: EMM failure	EMM failure.	Error	Put the system into maintenance mode
Dell - Storage: power supply failure	Power supply failure.	Error	Put the system into maintenance mode
Dell - Storage: temperature probe warning	Physical disk temperature probe warning, too cold or too hot	Warning	No action
Dell - Storage: temperature probe failure	Physical disk temperature probe error, too cold or too hot.	Error	Put the system into maintenance mode
Dell - Storage: Fan failure	Fan failure.	Error	Put the system into maintenance mode
Dell - Storage: Battery warning	Battery warning.	Warning	No action
Dell - Storage: Virtual disk degraded warning	Virtual disk degraded warning.	Warning	No action
Dell - Storage: Virtual disk degraded failure	Virtual disk degraded failure	Error	Put the system into maintenance mode
Dell - Storage: Temperature probe information	Temperature probe information	Info	No action
Dell - Storage: Array disk warning	Array disk warning.	Warning	No action
Dell - Storage: Array disk information	Array disk information.	Info	No action
Dell - Storage: Power supply warning	Power supply warning.	Warning	No action

A

Security Roles and Permissions

The OpenManage Integration for VMware vCenter stores user credentials in an encrypted format. It does not provide any passwords to client applications to avoid any improper requests that could lead to issues. The database back ups are fully encrypted using custom security phrases, and therefore the data cannot be misused.

By default, users in the Administrators group have all the privileges. Administrators can use all the functions of the OpenManage Integration for VMware vCenter within VMware vCenter. If you want a nonadmin user to manage the product, then create a role including both the Dell roles and then assign permission on the root/top node in the inventory and propagate permissions, as needed, on the child nodes to which you want to give access to the user. For example: if you want a user to manage only Cluster A, then keep the permissions on Cluster A and remove permissions from other clusters.

A

Data Integrity

Communication between the OpenManage Integration for VMware vCenter , Administration Console, and vCenter is accomplished using SSL/HTTPS. The OpenManage Integration for VMware vCenter generates an SSL certificate used for trusted communication between vCenter and the appliance. It also verifies and trusts the vCenter server's certificate before communication and the OpenManage Integration for VMware vCenter registration. OpenManage Integration for VMware vCenter Console tab (in VMware vCenter) uses security procedures to avoid improper requests while the keys are transferred back and forth from the Administration Console and back-end services. This type of security causes cross-site request forgeries to fail.

A secure Administration Console session has a five minute idle timeout, and the session is only valid in the current browser window and/or tab. If the user tries to open the session in a new window or tab, a security error is created that asks for a valid session. This action also prevents the user from clicking any malicious URL that could try to attack the Administration Console session.

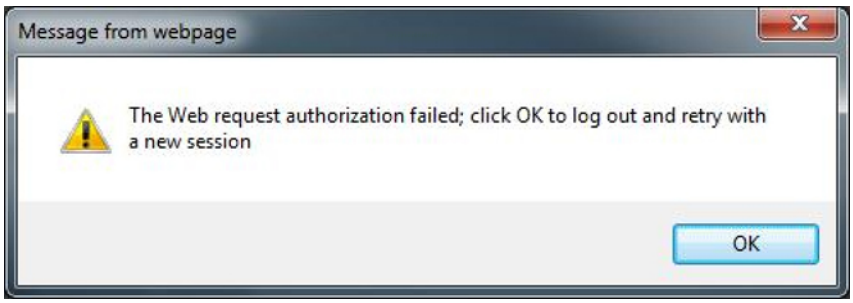

Figure 2. Error Message

A

Access Control Authentication, Authorization, and Roles

The OpenManage Integration for VMware vCenter uses the web Client's current user session and the stored administration credentials for the OpenManage Integration to perform vCenter operations. The OpenManage Integration for VMware vCenter uses the vCenter server's built-in roles and privileges model to authorize user actions with the OpenManage Integration and the vCenter managed objects (hosts and clusters). Access Roles on the VMware vCenter Home page.

A

Dell Operation Role

Contains the privileges/groups to accomplish appliance and vCenter server tasks including firmware updates, hardware inventory, restarting a host, placing a host in maintenance mode, or creating a vCenter Server task

This role contains the following privilege groups:

Privilege Group - Dell.Configuration	Perform Host-Related Tasks, Perform vCenter-Related Tasks, Configure SelLog, Configure ConnectionProfile, Configure ClearLed, Firmware Update
Privilege Group - Dell.Inventory	Configure Inventory, Configure Warranty Retrieval, Configure ReadOnly
Privilege Group - Dell.Monitoring	Configure Monitoring, Monitor
Privilege Group - Dell.Reporting (Not used)	Create a Report, Run a Report

A

Dell Infrastructure Deployment Role

This role contains the privileges specifically related to the hypervisor deployment features.

The privileges this role provides are Create Template, Configure HW Configuration Profile, Configure Hypervisor Deployment Profile, Configure Connection Profile, Assign Identity, and Deploy.

Privilege Group — Dell.Deploy — Provisioning	Create Template, Configure HW Configuration Profile, Configure Hypervisor Deployment Profile, Configure Connection Profile, Assign Identity, Deploy

A

Understanding Privileges

Every action performed by the OpenManage Integration for VMware vCenter is associated with a privilege. The following sections list the available actions and the associated privileges:

- Dell.Configuration.Perform vCenter-Related Tasks
  - Exit and enter maintenance mode
  - Get the vCenter user group to query the permissions
  - Register and configure alerts, for example enable/disable alerts on the event settings page
  - Post events/alerts to vCenter
  - Configure event settings on the event settings page
  - Restore default alerts on the event settings page
  - Check DRS status on clusters while configuring alerts/events settings
  - Reboot host after performing update or any other configuration action
  - Monitor vCenter tasks status/progress
  - Create vCenter tasks, for example firmware update task, host configuration task, and inventory task
  - Update vCenter task status/progress
  - Get host profiles
  - Add host to data center
  - Add host to cluster
  - Apply profile to host
  - Get CIM credentials
  - Configure hosts for compliance
  - Get the compliance tasks status
- Dell.Inventory.Configure ReadOnly
  - Get all vCenter hosts to construct the vCenter tree while configuring connection profiles
  - Check if the host is a Dell server when the tab is selected
  - Get the vCenter's Address/IP
  - Get host IP/Address
  - Get the current vCenter session user based on the vSphere client session ID
  - Get the vCenter inventory tree to display the vCenter inventory in a tree structure.
- Dell.Monitoring.Monitor
  - Get host name for posting the event
  - Perform the event log operations, for example get the event count, or change the event log settings
  - Register, unregister, and configure events/alerts – Receive SNMP traps and post events
- Dell.Configuration.Firmware Update
  - Perform firmware update
  - Load firmware repository and DUP file information on the firmware update wizard page

  - Query firmware inventory
  - Configure firmware repository settings
  - Configure staging folder and perform update using the staging feature
  - Test the network and repository connections
- Dell.Deploy-Provisioning.Create Template
  - Create, display, delete, and edit deployment templates
- Dell.Configuration.Perform Host-Related Tasks
  - Blink LED, Clear LED, Configure OMSA URL from the Dell Server Management tab
  - Launch OMSA Console
  - Launch iDRAC Console
  - Display and clear SEL log
- Dell.Inventory.Configure Inventory
  - Display system inventory in the Dell Server Management tab
  - Get storage details
  - Get power monitoring details
  - Create, display, edit, delete, and test connection profiles on the connection profiles page
  - Schedule, update, and delete inventory schedule
  - Run inventory on hosts

B

Understanding Auto-Discovery

Auto-Discovery is the process of adding a Dell PowerEdge 11th or 12th Generation bare-metal server into a pool of available servers for use by the OpenManage Integration for VMware vCenter. Once a server is discovered, use it for hypervisor and hardware deployment. This appendix provides sufficient information about Auto-Discovery to help you with system configuration. Auto-Discovery is a Lifecycle Controller feature for setting up a new server and registering it using a console. The advantages of using this capability include removing the need to do cumbersome manual local configuration of a new server and enabling an automated way for a console to discover a new server that was connected to the network and plugged into power.

Auto-Discovery is sometimes referred to as *Discovery and Handshake* after the process it performs. When a new server with the Auto-Discovery feature enabled is plugged in to AC power and connected to the network, the Dell server's Lifecycle Controller attempts to *discover* a deployment console that was integrated with the Dell provisioning server. Auto-Discovery then initiates a *handshake* between the provisioning server and the Lifecycle Controller.

OpenManage Integration for VMware vCenter is a deployment console with an integrated provisioning server. The location of the provisioning server is provided to the iDRAC using different methods. The IP address or host name for the provisioning server location is set to the IP address or host name of the OpenManage Integration for VMware vCenter appliance virtual machine.

NOTE: A new server configured for Auto-Discovery attempts to resolve the location of the provisioning server every 90 seconds over a period of 24 hours, after which you can manually reinitiate Auto-Discovery.

When the Auto-Discovery request is received by the OpenManage Integration for VMware vCenter for VMware vCenter, it validates the SSL certificate and then initiates any optionally configured security procedures, such as client side security certificates and validation against a white list. A second validation request from the new server returns temporary username/password credentials to be configured on the iDRAC. Subsequent calls are initiated by the OpenManage Integration for VMware vCenter for VMware vCenter, which gathers information about the server, remove the temporary credentials, and configure more permanent user-defined credentials for administrative access

If Auto-Discovery was successful, the deployment credentials provided in the Settings > Deployment Credentials page at the time of discovery are created on the target iDRAC. Then the Auto-Discovery feature is turned off. The server should now appear in the pool of available bare-metal servers under Deployment in the Dell Management Center.

Auto-Discovery can be currently done through the vSphere .Net client.

Auto-Discovery Prerequisites

Before attempting to discover Dell PowerEdge 11th or 12th Generation bare-metal servers, install the OpenManage Integration for VMware vCenter. Only Dell PowerEdge 11th Generation or later servers with iDRAC Express or iDRAC Enterprise can be discovered into the OpenManage Integration for VMware vCenter's pool of bare-metal servers. Network connectivity from the Dell bare-metal server's iDRAC to the OpenManage Integration for VMware vCenter virtual machine is required.

NOTE: Hosts with existing hypervisors should not be discovered into the OpenManage Integration for VMware vCenter, instead, add the hypervisor to a connection profile, and then reconciled with the OpenManage Integration for VMware vCenter using the Host Compliance Wizard

For Auto-Discovery to occur, the following conditions must be met:

- **Power:** Connect the server to the power outlet. The server does not need to be powered on.

- **Network connectivity:** The server's iDRAC must have network connectivity and must communicate with the provisioning server over port 4433. You can obtain the IP address using a DHCP server or manually specify it in the iDRAC Configuration Utility.
- **Additional network settings:** If using DHCP, enable the *Get DNS server address from DHCP* setting so that DNS name resolution can occur.
- **Provisioning service location:** The iDRAC must know the IP address or host name of the provisioning service server.
- **Account access disabled:** Enable the administrative account access to the iDRAC and if there are any iDRAC accounts with administrator privileges, first disable them from within the iDRAC web console. Once Auto-Discovery completes successfully, the administrative iDRAC account is re-enabled.
- **Auto-Discovery enabled:** The server's iDRAC must have Auto-Discovery enabled so that the Auto-Discovery process can begin.

Enabling or Disabling Administrative Accounts on iDRAC Servers

Before you can set up Auto-Discovery, disable all administrative accounts other than root. The root account is disabled during the Auto-Discovery procedure. Once you have successfully set up Auto-Discovery, return to the Integrated Dell Remote Access Controller 6 GUI and re-enable the accounts that were turned off. This procedure is for PowerEdge 11th and 12th generation servers.

NOTE: To guard against a failed Auto-Discovery, you may want to enable a non-admin account on the iDRAC. This allows remote access in the event the Auto-Discovery fails.

1. In a browser, type the **iDRAC IP address**.
2. Log in to the **Integrated Dell Remote Access Controller GUI**.
3. Do one of the following:
   - For iDRAC6: In the left pane, select **iDRAC Settings** → **Network/Security** → **Users** tab.
   - For iDRAC7: In the left pane, select **iDRAC Settings** → **User Authentication** → **Users** tab.
4. In the Users tab, locate any administrative accounts other than root.
5. To disable the account, under User ID, select the **ID**.
6. Click **Next.**
7. In the User Configuration page, under General, clear the **Enable User** check box.
8. Click **Apply**.
9. After you have successfully set up Auto-Discovery, to re-enable each account, repeat steps 1 to 8, but this time select the **Enable User** check box and click **Apply**.

Manually Configuring a PowerEdge 11th Generation Server for Auto-Discovery

You must have the iDRAC and host IP addresses.

If you have not ordered your bare metal appliance to use Auto-Discovery from the factory, you can set it up manually. iDRAC has two user interfaces, both are reached using the IP address of the iDRAC you want to set up.

On successful Auto-Discovery of bare-metal servers, the new administrator account is created or an existing account is enabled with the credentials returned by the handshake service. All the other administrative accounts that were disabled prior to Auto-Discovery will not be enabled. You must re-enable these administrator accounts after a successful Auto-Discovery. See Enabling or Disabling Administrative Accounts on iDRAC.

NOTE: If for some reason the Auto-Discovery did not complete successfully, there is no way to connect to the iDRAC remotely. Remote connection would require that you have enabled a non-admin account on the iDRAC. If there is no enabled account present on the iDRAC, then the only way to access the iDRAC is to login to the box locally and enabling the account on the iDRAC.

1. Enter the **iDRAC IP** address into a browser.
2. Log in to the **iDRAC Enterprise GUI**.
3. In the **Integrated Dell Remote Access Controller 6 — Enterprise** → **System Summary** tab, in the Virtual Console Preview, click **Launch**.
4. In the Warning — Security dialog, click **Yes**.
5. In the iDRAC Utility Console, press **F12** once or twice to bring up the Authentication Required dialog box.
6. In the Authentication Required dialog box, the name displays, press **Enter**.
7. Enter your **Password**.
8. Press **Enter**.
9. When the Shutdown/Restart dialog box appears, press **F11**.
10. The host restarts and the screen shows information about loading memory, then RAID, then when it shows iDRAC and says to press CTRL + E. Now, immediately press **CTRL + E**.

    If you see this dialog box, your action worked. If not, go to the Power menu and Power Off and Power On again and repeat this step.

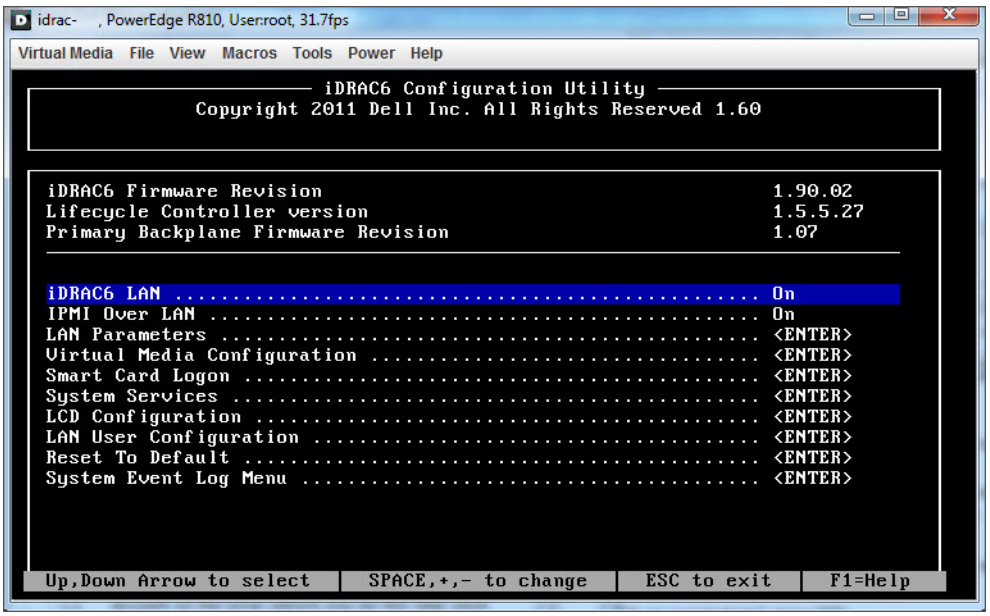
idrac- , PowerEdge R810, User:root, 31.7fps
Virtual Media File View Macros Tools Power Help
iDRAC6 Configuration Utility
Copyright 2011 Dell Inc. All Rights Reserved 1.60
iDRAC6 Firmware Revision 1.90.02
Lifecycle Controller version 1.5.5.27
Primary Backplane Firmware Revision 1.07
iDRAC6 LAN ..... On
IPMI Over LAN ..... On
LAN Parameters ..... <ENTER>
Virtual Media Configuration ..... <ENTER>
Smart Card Logon ..... <ENTER>
System Services ..... <ENTER>
LCD Configuration ..... <ENTER>
LAN User Configuration ..... <ENTER>
Reset To Default ..... <ENTER>
System Event Log Menu ..... <ENTER>
Up,Down Arrow to select
SPACE,+,- to change
ESC to exit
F1=Help

Figure 3. Press CTRL + E to activate this screen.

11. In the iDRAC6 Configuration Utility, use the arrow keys to select **LAN Parameters**.
12. Press **Enter**.
13. If this host is a blade, to configure NIC, use the space bar to toggle the options to **Enabled**.
14. If you are using DHCP, use the arrow keys to select **Domain Name from DHCP**.
15. Use the space bar to toggle the option to **On**.
16. If you are using DHCP, use the arrow keys to navigate to the IPv4 settings and select **DNS Servers from DHCP**.
17. Use the spacebar to toggle the option to **On**.

18. To Exit, on your keyboard, press **ESC**.
19. Use the arrow keys to select **LAN User Configuration**.
20. Use the arrow Keys to select **Provisioning Server**.
21. Press **Enter**.
22. Enter the IP address of the host.
23. Press **ESC**.
24. Use arrow keys to select **Account Access**.
25. Use the space bar to toggle the option to **Disable**.
26. Use the arrow keys to select **Auto-Discovery**.
27. Use the space bar to toggle the option to **Enabled**.
28. From your keyboard, press **ESC**.
29. Press **ESC** again.

Manually Configuring a PowerEdge 12th Generation Server for Auto-Discovery

You must have the iDRAC and host IP addresses.

If you have not ordered your bare metal appliance to use Auto-Discovery from the factory, you can set it up manually. iDRAC has two user interfaces, both are reached using the IP address of the iDRAC you want to set up.

On successful Auto-Discovery of bare-metal servers, the new administrator account is created or an existing account is enabled with the credentials returned by the handshake service. All the other administrative accounts that were disabled prior to Auto-Discovery are not enabled. Re-enable these administrator accounts after a successful Auto-Discovery. See Enabling or Disabling Administrative Accounts on iDRAC.

NOTE: If for some reason the Auto-Discovery did not complete successfully, there is no way to connect to the iDRAC remotely. Remote connection would require that you have enabled a nonadmin account on the iDRAC. If there is no enabled account present on the iDRAC, then the only way to access the iDRAC is to login to the box locally and enabling the account on the iDRAC.

1. Enter the **iDRAC IP address** into a browser.
2. Log in to the **iDRAC Enterprise GUI**.
3. In the **Integrated Dell Remote Access Controller 7— Enterprise → System Summary** tab, in the Virtual Console Preview, click **Launch**.
4. In the Warning — Security dialog, click **Yes**.
5. In the iDRAC Utility Console, press **F12** once or twice to bring up the Authentication Required dialog box.
6. In the Authentication Required dialog box, the Name displays, press **Enter**.
7. Enter your **Password**.
8. Press **Enter**.
9. When the Shutdown/Restart dialog box appears, press **F11**.
10. The host restarts and the screen shows information about loading memory, then RAID, then when it shows a Dell screen where it says to press F2, immediately press **F2**.

    Wait until the Dell System Setup screen displays. The Dell System Setup takes a few minutes to display.
11. In the Dell System Setup screen use the arrow keys to select **iDRAC Settings**.
12. Use the arrow keys to select **Remote Enablement**.
13. To enable Auto-Discovery, click **Enable**.
14. Press **ESC**.

15. Press **ESC**.
16. In the Warning Screen, to confirm Exit, click **Yes**.